UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
A R A G Ó N

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE CALIDAD EN SEGURIDAD DE LA INFORMACIÓN SGSI

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN

P R E S E N T A:

OMAR NICASIO CHAVEZ

DIRECTOR DE TESIS:
Ing. Rodolfo Vázquez Morales
2015

Impresión: México DF Mayo 2015

DESARROLLO DE TEMA PARA TITULACIÓN BASADO EN EL DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE CALIDAD EN SEGURIDAD DE LA INFORMACIÓN SGSI.

CAPITULO 1.- SISTEMA DE GESTION DE CALIDAD.

1. ¿Qué es el sistema de gestión de calidad en seguridad de la información o SGSI?
   - 1.1. ¿Qué es el SGSI?
   - 1.2. ¿Para qué sirve?
   - 1.3. ¿Qué incluye el SGSI?
   - 1.4. ¿Cómo se implementa un SGSI?
2. ¿Qué ISOS están relacionados?
   - 2.1. ¿Interrelación entre sí?
3. ¿Qué relación tiene la calidad vs informática en las empresas?
4. ¿Qué aspectos empresariales de informática relacionados con la informática pueden mejorarse con “SGSI”?
5. Metodología
   - 5.1. Metodología por etapas

CAPITULO 2.- PROCESO DE DISEÑO E IMPLEMENTACION DEL SGSI.

1. ¿Qué es MAAGTIC?
2. ¿Qué contiene el MAAGTIC?
3. Alcance del MAAGTIC
4. ¿Y cuál es el reto de las empresas que prestan servicios al gobierno y estar alineados al MAAGTIC?
5. Pero de que depende el éxito para logar el alineamiento con el MAAGTIC
6. Presentación del proyecto

CAPITULO 3.- RESULTADOS Y SOLUCIONES DADOS POR EL SGSI.

1. Análisis externo, Reporte ejecutivo y Análisis de vulnerabilidades
   - 1.1. Introducción
   - 1.2. Objetivo
   - 1.3. Herramientas y técnicas
   - 1.4. Alcance
   - 1.5. Análisis de vulnerabilidades
   - 1.6. Top de vulnerabilidades
   - 1.7. Servicios vulnerables
   - 1.8. Estado de vulnerabilidades
   - 1.9. Índice de vulnerabilidades
   - 1.10. Evidencia de vulnerabilidades
   - 1.11. Anexo
     - 1.11.1. Detalle técnico de cada uno de los activos

2. Análisis interno, Reporte ejecutivo y Análisis de vulnerabilidades

Contenido

AGRADECIMIENTOS

A mis padres *REFUGIO Y LAURA*:

Mamá, Papá muchas gracias por todo lo que han hecho por mí, ustedes son mi más grande orgullo y el principal motivo para seguir adelante, gracias por su tiempo, sus enseñanzas, su educación, el apoyo, los consejos, el cariño, los regaños y el amor que me dan, por los valores que me han inculcado, por enseñarme a luchar para conseguir y hacer realidad mis metas y sueños, por darme la mano cuando sentía que todo estaba perdido, porque gracias a todo eso he llegado hasta donde estoy y me motiva a ser cada día mejor persona y mejor ser humano, los amo enormemente. Recuerden que este logro en mi vida es en gran parte SUYO, MUCHAS GRACIAS LOS AMO MUCHO.

A mis hermanas *VERONICA y DIANA*:

Que con su gran amor y apoyo me han enseñado que todo es mucho mejor unidos, y que no importa que tan oscura sea la noche siempre me estarán ahí para apoyarme, muchas gracias por su paciencia y consejos y por siempre preocuparse por mí, muchas gracias por compartir conmigo esta etapa tan importante en mi vida.

A mis abuelos *ADELA †, TRANQUILINO †, LUISA † y ALFONSO*:

Gracias porque siempre supieron inculcar e influir en mí su sabiduría, su experiencia, sus valores, sus consejos y con ello al igual que lo hicieron con mis padres con sus enseñanzas y apoyo para ser mejor cada día, a los que ya no se encuentran con nosotros, donde estén esta meta también es suya.

Abuelo Alfonso muchas gracias por escucharme y apoyarme.

A mis Amigos

A todos mis amigos y compañeros para no excluir a nadie, muchas gracias por brindarme ese sentimiento que es la amistad y hermandad, por compartir conmigo tantas horas de estudio como de diversión, por la ayuda y los consejos.

Al Ing. *Rodolfo Vázquez Morales*:

Antes que nada te agradezco mucho tu amistad que siempre me has brindado, el apoyo incondicional, los consejos tanto académicos, profesionales y personales, las horas de clase que fueron de gran calidad y que gracias al empeño y dedicación con la que las impartes, me ayudaron mucho a encontrar el área que más me agrada la seguridad de la información, y sobre todo gracias por apoyar y ser partícipe de este proyecto de titulación.

A los revisores de tesis:

Muchas gracias por todo el apoyo, por su disposición y ayuda al leer mi trabajo de tesis, por sus observaciones, sugerencias y correcciones a él.

A la **UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO**

Que me brindó la oportunidad de crecer personal y profesionalmente, por permitir pertenecer a esta gran comunidad, por haber recibido de ella mi formación profesional, por los excelentes profesores de los que tuve la oportunidad de aprender.
POR MI RAZA HABLARA EL ESPIRITU.

Son muchas más a las personas a las que me gustaría agradecer su amistad, apoyo, ánimo y compañía en las diferentes etapas de mi vida. Algunas están aquí conmigo y otras en mis recuerdos y en el corazón. Sin importar donde estén o si alguna vez llegan a leer estas estas dedicatorias quiero darles las gracias por formar parte de mi vida, por todo lo que me han brindado y por todas sus bendiciones.

OMAR NICASIO CHÁVEZ

AGRADECIMIENTOS DEL ASESOR

Omar:

Muchas gracias por hacerme partícipe de tú proyecto, pero sobre todo por brindarme lo más importante que podemos tener los seres humanos, amistad. Te deseo una vida plena y llena de triunfos profesionales, pero sobre todo personales, fuerza amigo!

A nuestros revisores:

Gracias por mejorar y enriquecer el proyecto, como siempre es un placer trabajar con ustedes.

Dr. Carlos Eduardo Levy Vázquez † :

En mi vida he tenido la fortuna de convivir con mucha gente que ha contribuido con lo que soy, usted es una de las más trascendentales y hablo en presente porque en cada lugar de nuestra universidad hay una enseñanza que me recuerda lo que usted fue, es y será.

Fue muy difícil empezar el semestre 2014-2 sabiendo que usted no estaría, solo me queda darle las gracias por las pláticas, por siempre mirar a los ojos, por su entusiasmo, por la pasión y enseñarme que siempre podemos confiar y especialmente en los jóvenes. Con el mayor de mis respetos a un Universitario sin igual pero a un mejor ser humano. Se le extraña Dr. Carlos.

M. en C. Ricardo Gutiérrez Orozco:

Hace 21 años curse la materia de Sistemas Operativos teniéndolo como mi profesor, desde entonces he tenido la dicha de convivir con usted por lo menos tres minutos cada semana.

Hoy quiero agradecerle tres cosas, primero todo lo que me enseño en la materia porque administrar servidores es uno de mis más grandes gustos; segundo el gran sentido de responsabilidad que siempre debo tener, y tercero a siempre estar dispuesto a colaborar con quien nos lo pide. Gracias por todo, lo quiero y respeto.

Ing. José Antonio Ávila García:

De las muchas materias que tuve en la licenciatura, hubo una que me hizo entender la vida de distinta manera, fue Calidad. Hubo dos razones fundamentales, primero el contenido de la materia y segundo el gran profesor que la impartió, usted.

Nunca se lo he dicho pero hoy tengo la necesidad de hacerlo, porque con la excelente cátedra que recibí de usted, me ayudo a desarrollarme de forma diferente pudiéndolo aplicar en todo lo que hago, laboral y personalmente. Gracias, lo quiero y admiro.

Universidad Nacional Autónoma de México:

Solo me resta decir que no hay mejor lugar en el mundo, “Por mi raza hablara el espíritu”.

Ing. Rodolfo Vázquez Morales

INTRODUCCION

Este trabajo de investigación que realizo es para poder obtener el título de Ingeniero en computación. Dicho trabajo de investigación es basado en el área de seguridad de la información que hoy en día es una de las principales e importantes áreas en empresas tanto públicas como privadas.

El área de seguridad se encarga de vigilar, monitorear el comportamiento de los sistemas, resguardar los activos y pasivos informáticos que maneja y por ende si estos sufrieran algún incidente o afectación ya sea física o lógica se estaría poniendo en juego la competitividad, la estabilidad, la continuidad de la empresa y en un caso extremo su permanencia en el mundo empresarial por la pérdida de información tiempo y recursos financieros lo que es vital.

Todas las empresas tienen problemas con sus tecnologías de la información esto repercute en afectaciones en su operación cotidiana en servidores, sistemas, redes, servicios y aplicaciones.

Existen varias alternativas para solucionar lo anterior, sin embargo sugerimos por la experiencia adquirida en servicio social la implementación de un Sistema de Gestión de Seguridad de la Información “SGSI” por ser un sistema más integral además de dar una solución más completa a la seguridad de la empresa y por ende seguir asegurando la continuidad y su correcta operación cotidiana.

Y es en este trabajo de investigación a lo largo de sus capítulos se podrá adentrar y apreciar el cómo se gestiona la seguridad de la información, que estándares la rigen, que indicadores y controles se aplican y que metodología se sigue y en una manera general como es que en sí es la estructura del Sistema de Gestión de la Seguridad de la Información (SGSI).

NOTA:

POR MOTIVOS DE ETICA PROFESIONAL E INTEGRIDAD DE LA INFORMACION SE OMITEN LOS NOMBRES DE LAS EMPRESAS DE LAS CUALES FUE TOMADA LA INFORMACION Y LOS RESULTADOS PARA LA REALIZACION DE ESTA TESIS.

DE AQUÍ EN ADELANTE SE LE DENOMINARA A LA EMPRESA PRESTADORA DEL SERVICIO DE REVISION DEL SGSI COMO **CONSULTOR REVISOR DEL SGSI**, A LA EMPRESA ENCARGADA DE LOS RESULTADOS CONSULTOR DE RESULTADOS Y A LA EMPRESA RECEPTORA COMO **ORGANISMO RECEPTOR**.

C A P I T U L O 1

SISTEMA DE GESTION DE CALIDAD EN SEGURIDAD DE LA INFORMACION O SGSI

CAPITULO 1.- SISTEMA DE GESTION DE CALIDAD (SGSI)

¿QUÉ ES EL SGSI?

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

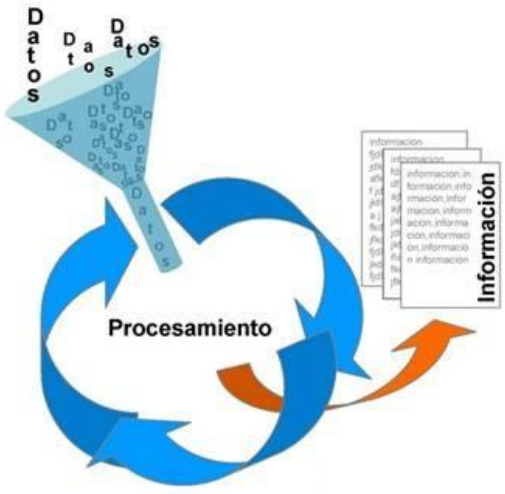
Un Sistema de Gestión de la seguridad de la Información (SGSI) es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido. El término es utilizado principalmente por la ISO/IEC 27001.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso en el que se dispusiera de un presupuesto ilimitado, es por esto que el propósito del SGSI es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, minimizados y gestionados de una forma documentada, sistemática, estructurada, repetible, eficiente, y adaptable a los cambios que se produzcan en los riesgos, en el entorno y en las tecnologías.

El concepto clave de un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar correcta y eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

- *Confidencialidad:* La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- *Integridad:* Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- *Disponibilidad:* Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.



¿PARA QUÉ SIRVE?

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

La protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo.

El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

¿QUÉ INCLUYE UN SGSI?

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma:

- **Documentos de Nivel 1**

Manual de seguridad: Por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

- **Documentos de Nivel 2**

Procedimientos: Documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

- **Documentos de Nivel 3**

Instrucciones, checklists y formularios: Documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

- **Documentos de Nivel 4**

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

- Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).
- Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.
- Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.
- Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
- Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

- Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.
- Registros: documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.
- Declaración de aplicabilidad: (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

¿CÓMO SE IMPLENTA?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información por lo regular se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

- **Plan (planificar):** Establecer el SGSI.

En esta etapa se define el alcance que tendrá el Sistema de Gestión de Seguridad de la Información (SGSI) en términos del negocio, de la organización en donde se incluyen detalles y las justificaciones.

Se define la política de seguridad en la cual se tiene que incluir:

- El marco general y los objetivos de dicha política de seguridad de la organización.
- Se consideran los requerimientos legales, contractuales u organizacionales relativos a la seguridad de la información.
- Se debe alinear a la estrategia de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI.
- Sobre todo que la dirección este de acuerdo y apoye el SGSI.

Se debe definir una metodología apropiada para el SGSI y para la organización en cuanto a las necesidades del negocio eso es tan importante ya que todo depende de los resultados que arroje la metodología, estos deben ser comparables y repetibles, además de definir los criterios aceptación de riesgos y especificar el nivel de riesgo aceptable.

Se deben Identificar los riesgos en la organización se deben de identificar los activos y a sus responsables directos que estén dentro del alcance del SGSI, identificar las amenazas y las vulnerabilidades que pueden ser explotadas y así mismo identificar que o cual es el impacto a la integridad, disponibilidad y confidencialidad.

Se analizan y evalúan los riesgos y el impacto en el negocio que pueda derivar en una perdida en la confidencialidad integridad o disponibilidad en la información y evaluar de forma realista y fehaciente la probabilidad de ocurrencia en el fallo de la seguridad o de los riesgos en relación a las amenazas, vulnerabilidades e impactos a los activos de la organización y a los controles implementados.

Se estiman los niveles de riesgo y se determina en base a los criterios de aceptación si el riesgo es realmente aceptable o se requiere que sea tratado y para poder identificar y evaluar los riesgos hay varias opciones:

- Se aplican los controles adecuados.
- Se acepta el riesgo siempre y cuando se estén cumpliendo las políticas, lineamientos y criterios para la aceptación de los riesgos.
- Evitar el riesgo en la medida de lo posible.
- Transferir el riesgo a terceros (aseguradoras o proveedores de outsourcing).

Se seleccionan los objetivos de control y los controles para el tratamiento que cumplan con los requerimientos identificados en el proceso de la evaluación de los riesgos.

Se debe aprobar por parte de la dirección tanto los riesgos, la implantación y el uso del SGSI.

Se debe definir la declaración de aplicabilidad en la que se incluya:

- Los objetivos de control, los controles seleccionados y los motivos para su elección
- Los objetivos de control y los controles que se encuentran implantados
- Los objetivos de control y los controles excluidos y los motivos de la exclusión, este es un mecanismo que nos permite identificar posibles omisiones involuntarias

- **Do (hacer):** Implementar y utilizar el SGSI.

Se define un plan de tratamiento de riesgos en el que se pueda identificar las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de la seguridad de la información.

Implantar el plan de tratamiento de riesgos con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

Implementar los controles que se seleccionaron anteriormente que lleven a los objetivos de control.

Se define un sistema de métricas que nos permita obtener resultados reproducibles y comparables para medir el comportamiento y la eficacia de los controles o grupos de controles implementados.

Procurar tener programas de formación y concienciación para el personal en relación a la seguridad de la información.

Gestionar las operaciones y los recursos necesarios asignados para el mantenimiento del SGSI.
Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

- **Check (verificar):** Monitoreo verificación y revisión del SGSI.

En esta parte la organización deberá:

Ejecutar procedimientos para el monitoreo y revisión para:

- Detectar a tiempo los errores en los resultados generados por el procesamiento de la información.
- Identificar brechas e incidentes de seguridad.
- Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores.
- Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

Revisar regularmente la efectividad del SGSI, ver el cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

Medir la efectividad de los controles para verificar que el cumplimiento con los requisitos de seguridad.

Revisar regularmente en intervalos planeados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior tales como los requerimientos legales, obligaciones contractuales, etc.-.

Realizar periódicamente auditorías internas del SGSI en intervalos periódicos y continuos.

Revisión periódica del SGSI por parte de la dirección para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.

Actualizar los planes de contingencias de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitoreo y revisión.

Registro de acciones y eventos que pudieran y pueden haber impactado sobre la efectividad o el rendimiento del SGSI.

- **Act (actuar):** Mantener y mejorar el SGSI.

En esta etapa regularmente la organización debe regularmente:

Implantar en el SGSI las mejoras identificadas.

Realizar las acciones preventivas y correctivas adecuadas obtenidas en base a las lecciones aprendidas de las etapas anteriores y en base a las experiencias propias y de otras organizaciones.

Comunicar las acciones y las mejoras a todas y cada una de las partes interesadas con el nivel de detalle adecuado para acordar y si es pertinente, la forma de proceder.

Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

El Plan→Do→Check→Act (PDCA) es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases.
Se debe tomar en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, por ejemplo, puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

¿QUÉ ISOS ESTAN RELACIONADOS?

La información es un activo vital para el éxito y la continuidad de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por lo tanto, uno de los objetivos primordiales para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en objetivos claros de seguridad y una evaluación de los riesgos a los que se encuentra expuesta la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

A continuación hago un pequeño resumen de las distintas normas que nos indican el cómo se puede organizar, implantar o mejorar un sistemas de gestión de seguridad de la información (SGSI) basado en la serie de estándares 27000

En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001.

1. Los ISO relacionado a este sistema son los de la familia 27000 pero los principales son los que se enlistan a continuación:
   - El ISO 27001 es un estándar para la seguridad de la información denominado ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) adoptado por ISO, basado en un estándar británico denominado BS 7799. Es certificable y su primera publicación fue en el año 2005. En éste se determinan los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) a través del ciclo de Deming-PHVA por medio de los procesos de planificar, hacer, verificar y actuar.
   - El ISO 27002 se trata de una guía de buenas prácticas a partir de objetivos de control y controles recomendables a nivel de seguridad de la información. A diferencia de ISO 27001, no es un estándar certificable. Cuenta con 39 objetivos de control y 133 controles agrupados en 11 dominios, abordando más controles y dominios que los establecidos en el estándar certificable ISO 27001

   - El ISO 27005 se trata de un estándar internacional denominado ISO 27005:2008, Information technology – Security Techniques – Information Security Risk Management. Fue creado en el año 2008 y provee pautas para la gestión del riesgo de seguridad de la información. Como procedimiento vital, al hablar de seguridad de la información aparece el análisis, evaluación y gestión de los riesgos, por ello este documento ilustra un marco de referencia para el tratamiento de las actividades antes mencionadas.

2. El IT CobiT, este documento establece un marco de trabajo basado en dominios y procesos, a través del cual se ofrecen unas buenas prácticas enfocadas a optimizar la inversión de recursos en áreas de TI, brindando así calidad, gestión y correcta administración en los servicios prestados, abordando también, temas de seguridad asociados a los servicios.

   CobiT se estructura en cuatro partes; la principal de ellas se divide de acuerdo con 34 procesos de TI. Cada proceso se cubre en cuatro secciones (objetivo de control de alto nivel para el proceso, los objetivos de control detallados, directrices de gestión y el modelo de madurez para el objetivo) que dan una visión completa de cómo controlar, gestionar y medir el proceso. Utiliza un ciclo de vida de tipo PDCA que lo integra en los procesos de negocio.

   No existe un certificado en las prácticas indicadas por CobiT, aunque ISACA sí ofrece la posibilidad a título personal de obtener certificaciones como “Certified Information Systems Auditor” (CISA), “Certified Information Security Manager” (CISM) y "Certified in the Governance of Enterprise IT"CGEIT.

3. El compendio de documentos de ITIL “IT Infrastructure Library”, conocido como la Biblioteca de Infraestructura de Tecnologías de Información para las mejores prácticas en la gestión de servicios TI, aborda recursos orientados a la correcta gestión de los servicios de TI a través de un ciclo de vida de los servicios, evaluando inmerso en cada una de las fases del ciclo temas de seguridad, capacidad y continuidad.

   Las áreas cubiertas por ITIL en cada documento publicado por la OGC son:

- Soporte al servicio: asegurar que el cliente (externo o interno) recibe adecuadamente un servicio, que es gestionado además de la mejor forma posible.
- Entrega del servicio: administración de los servicios de soporte y mantenimiento que se prestan al cliente.
- Planificación de la implantación: determina las ventajas de implantar ITIL en una determinada organización.
- Administración de aplicaciones: conjunto de buenas prácticas para la gestión de todo el ciclo de vida de las aplicaciones, centrándose sobre todo en definición de requisitos e implementación de soluciones.
- Administración de la infraestructura de tecnologías de la información y comunicaciones: gestión de la administración de sistemas como máquinas, redes o sistemas operativos, entre otros.
- Administración de seguridad: proceso para la implantación de requerimientos de seguridad; relaciona las áreas ITIL de soporte y entrega de servicio.
- Administración de activos de software: pautas necesarias para la gestión del software adquirido y/o de desarrollo propio.
- Entrega de servicios desde un punto de vista de negocio: fidelización de clientes, servicios de externalización y gestión del cambio, entre otros.

Actualmente existe una nueva versión ITIL V3 que fue publicada en mayo de 2007 que incluye cinco libros principales, concretamente: Diseño de Servicios de TI, Introducción de los Servicios de TI, Operación de los Servicios de TI, Mejora de los Servicios de TI y Estrategias de los Servicios de TI, consolidando buena parte de las prácticas actuales de la versión 2 en torno al Ciclo de Vida de los Servicios.

4. En este documento (NIST SP 800-30) contiene una guía desarrollada por el National Institute of Standards and Technology (NIST). “Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of standards and Technology”. Este documento fue creado en el año 2002 y ofrece pautas para la gestión del riesgo buscando su evaluación, gestión, control y mitigación. A través de este documento, en conjunto con ISO 27005, es posible identificar y establecer métodos a través de los cuales gestionar los riesgos identificados en una organización, diseñar y aplicar controles para la correcta mitigación de estos.

5. BS 25999 en este estándar de origen británico, aborda los lineamientos que deben contemplarse para la administración de la continuidad del negocio. A través de 2 partes. La primera ofrece un marco de referencia para procesos, principios y terminología asociado a la continuidad del negocio. En la segunda, se encuentran los requerimientos para implementar, operar y mejorar un sistema de administración de la continuidad del negocio.

Con origen en PAS 56:2003, BS 25999-1 establece el proceso por el cual una organización puede desarrollar e implementar la continuidad de negocio, incluyendo una completa lista de controles basada en las mejores prácticas de BCM (Business Continuity Management). Está pensada para su uso por cualquier organización grande, mediana o pequeña, tanto del sector público como privado.

En 2007, fue publicada BS 25999-2, que especifica los requisitos para establecer, implementar, operar, supervisar, revisar, probar, mantener y mejorar un sistema de gestión de continuidad de negocio documentado en el contexto de la gestión global de riesgos de

una organización. En base a esta norma pueden ser certificados los sistemas de gestión de continuidad de negocio.

Existe una traducción de las partes 1 y 2 publicadas en español y denominadas "UNE 71599-1:2010 Gestión de la continuidad del negocio. Código de práctica" y "UNE 71599-2:2010 Gestión de la continuidad del negocio. Especificaciones" y disponibles para su adquisición conjunta desde la página de AENOR.

INTERACION ENTRE SÍ

Lograr una alineación entre los documentos antes indicados tiene un alto grado de dificultad, pero a la vez es una gran oportunidad para crear un conjunto de métodos y procedimientos complementarios que abarquen gran cantidad de puntos, lográndose uno a uno el aseguramiento de los activos, los procesos y los recursos tecnológicos de la organización. Además, permiten crear consciencia en la importancia de la seguridad de la información al personal que forma parte de la organización

1. Relación que tiene la calidad vs Informática en las empresas

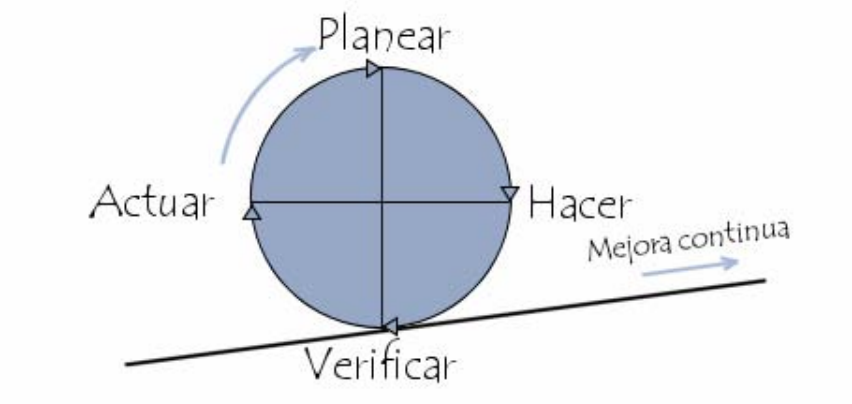
La palabra "calidad" se usa cada vez con más frecuencia en las empresas, ya sea en los sectores de alimentos, industria o servicios y especialmente en el sector de Tecnología Informática (TI).

La Calidad se puede definir como la capacidad de lograr objetivos de operación buscados o como el conjunto de características de una entidad que le otorgan la capacidad de satisfacer necesidades expresas e implícitas.

Es cuestión de encontrar el equilibrio correcto que elimine los defectos de calidad lo mejor posible para ganar un buen grado de satisfacción y lealtad del cliente y para generar ganancias, todo dentro de un presupuesto razonable.

Mejoras continuas

Uno de los principios básicos de la calidad es la prevención y las mejoras continuas. Esto significa que la calidad es un proyecto interminable, cuyo objetivo es detectar disfunciones tan rápido como sea posible después de que ocurran. Así, la calidad puede representarse en un ciclo de acciones correctivas y preventivas llamado "ciclo de Deming":



Este ciclo, representado en el ciclo de Deming, se llama modelo PDCA. PDCA se refiere a las iniciales del inglés de los siguientes cuatro pasos:

- Planear (plan): definir los objetivos a alcanzar y planificar cómo implementar las acciones
- Hacer (do): implementar las acciones correctivas
- Controlar (check): verificar que se logre el conjunto de objetivos
- Actuar (act): según los resultados obtenidos en el paso anterior, tomar medidas preventivas

La calidad juega un papel muy importante en las empresas sobre todo en el área informática ya que ella depende mucho de la calidad del trabajo, los procesos, los procedimientos, la manipulación, en el manejo de la información.

ASPECTOS INSTITUCIONALES QUE PUEDEN MEJORARSE CON EL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION

En este caso me basare en el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones (MAAGTIC) que es un documento emitido por el Gobierno de los Estados Unidos Mexicanos por la Secretaria de la Función Pública.

Este documento tiene como objetivo general definir los procesos que en materia de TIC regirán hacia el interior de la Unidad de Tecnologías de la Información y Comunicaciones (UTIC), con el propósito de lograr la cobertura total de la gestión, de manera que, independientemente de la estructura organizacional con que cuenten o que llegaran a adoptar; los roles definidos puedan acoplarse a los procesos establecidos para lograr la cohesión total para una mejor gestión.

Y los objetivos específicos:

1. Proporcionar a las Instituciones procesos simplificados y homologados en materia de TIC, así como las correspondientes regulaciones para cada proceso.
2. Establecer indicadores homologados que permitan a la SFP medir los resultados de la gestión de la UTIC de manera que le sea posible definir estrategias de apalancamiento y apoyo a las Instituciones que lo requieran.
3. Contribuir, mediante la aplicación generalizada del Marco rector de procesos en materia de TIC, a alcanzar una mayor eficiencia en las actividades y procesos institucionales e interinstitucionales, a partir del quehacer orientado al servicio y satisfacción del ciudadano.

METODOLOGÍA

La metodología debe ser respaldada por un proceso formal que asegure su previo entendimiento por cada uno de los responsables de llevar a la práctica dicho proceso en la empresa. Al igual que otras funciones en el negocio, la metodología efectúa sus tareas y actividades mediante un proceso definido.

Es importante señalar que el uso de la metodología no garantiza por si sola el éxito de los proyectos de auditoria en informática; además se requiere un buen dominio y uso constante de los siguientes aspectos complementarios.

Hay que cuidar muy bien las fronteras de la función de auditoria informática y delegar las responsabilidades a quien corresponda.

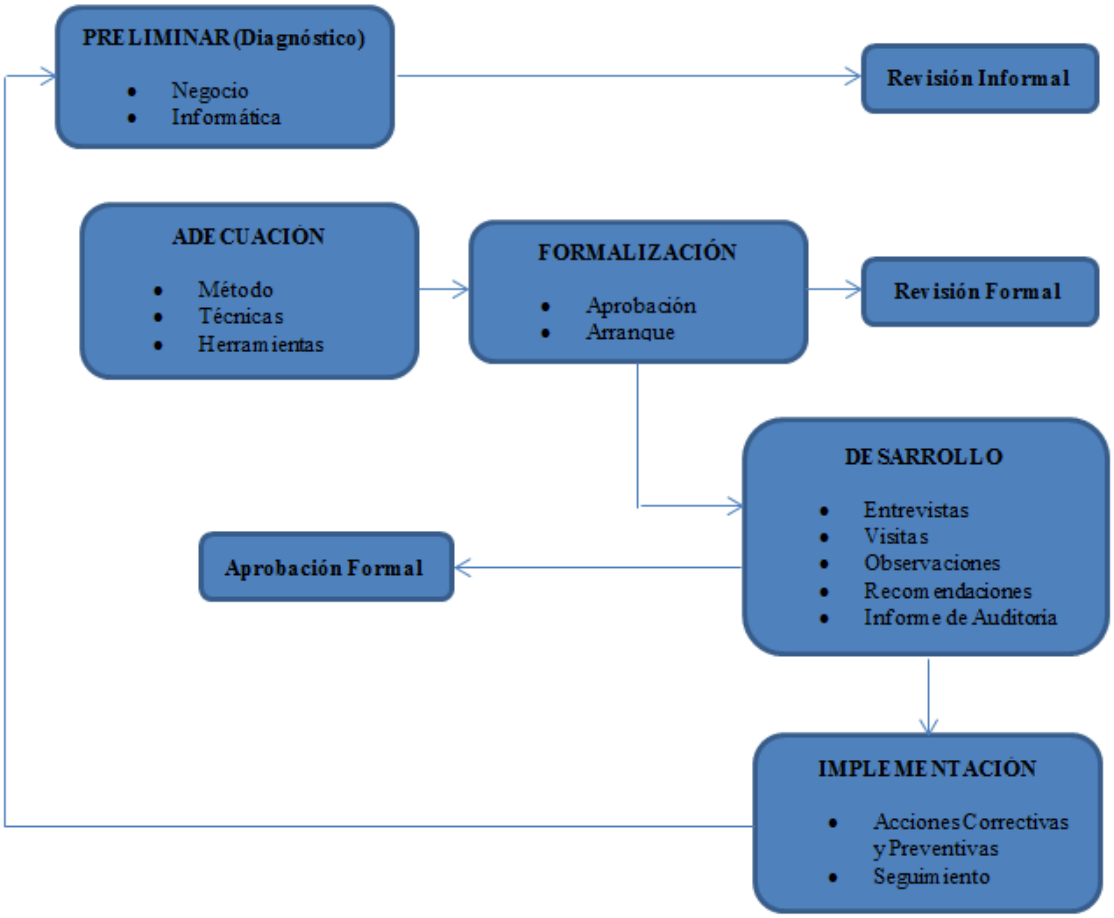


TABLA GENERAL: *Tareas, productos, responsables e involucrados*

ETAPA	PRODUCTOS TERMINADOS	REQUERIMIENTOS	RESPONSABLE	INVOLUCRADOS
PRELIMINAR (diagnóstico)	1. Diagnóstico de negocio	Involucramiento de la dirección	LP	AD / AI
	2. Diagnóstico de informática	Información veraz	LP	RI / RAI
ADECUACIÓN	1. Plan y metodología de acuerdo con el cliente	Entendimiento del negocio y de la función de informática	LP	RI / RAI / PU
	2. Plan detallado	Detallar tareas y tiempos	AI	RI / RAI / PU
FORMALIZACIÓN	1. Plan aprobado	Aprobación formal (firmas)	AD	RI / RAI / PU
	2. Compromiso ejecutivo	Respaldo y apoyo al proyecto	AD	RI / RAI / PU
DESARROLLO	1. Auditar áreas seleccionadas	Aprobación de la dirección	LP	RI / PU / AI
	2. Informe de auditoría en informática	Asignar responsables y tiempos para cada acción recomendada	AD / PI / PU	RAI / LP / AI
IMPLANTACIÓN	1. Recomendaciones y acciones terminadas	Compromiso ejecutivo	RI / PU	LP / AI
	2. Aprobación final	Basarse en plan de implantación Verificar cumplimiento del plan	LP / AI	RI / PU / RAI

Nomenclatura: AD = alta dirección; PU = personal usuario; RI = responsable del área de informática; PI = personal de informática; RAI = responsable del área de auditoría en informática; LP = líder del proyecto de auditoría en informática; AI = auditor en informática

METODOLOGÍA POR ETAPAS

ETAPA PRELIMINAR (diagnóstico)

Es el primer paso práctico dentro de la empresa o institución al efectuar la auditoria informática y es posible detectar las fortalezas, aciertos y apoyo que brinda dicha función desde la perspectiva de los directivos del negocio.

Es conveniente aclarar que no se debe tratar esta etapa como un conjunto de tareas que requiere muchos recursos ni un tiempo considerable; simplemente es un aspecto necesario y generalizado para entender los puntos débiles y fuertes de la función de informática desde un punto de los usuarios clave y la alta dirección.

Todas las actividades deben estar claramente definidas en todos los componentes formales que integran cualquier trabajo dentro de una organización.

No hay que confundir la fase preliminar con la fase de desarrollo e implementación; en la primera el estudio es corto en tiempo y general en su investigación. Se menciona aprovechar las áreas de oportunidad que no requieren la terminación de la auditoria informática para comenzar su implantación. Es conveniente recordar que se carece de mucho soporte documental y detallado en este momento, por lo que la sugerencia de áreas de oportunidad utópicas puede crear cierta incredulidad y rechazo hacia el auditor en informática.

ETAPA	TAREAS	PRODUCTOS	REPONSABLE	INVOLUCRADOS
PRELIMINAR (Diagnóstico)	1. Diagnóstico de negocio	1.1. Misión y objetivos de negocio	LP / RAI	AD
		1.2. Organización de informática	LP / RAI	AD
		1.3. Grado de apoyo al negocio	LP / RAI	AD / PU
	2. Diagnóstico de informática	2.1. Misión y objetivos de la función informática	LP / RAI	RI
		2.2. Organización de informática	LP / RAI	RI
		2.3. Control (formalidad)	LP / RAI	RI / PI
		2.4. Productos y servicios	LP / RAI	RI
	3. Detectar área de oportunidad	3.1. Área de oportunidad para mejoras inmediatas	LP / RAI	AD / PU / RI

Nomenclatura: AD = alta dirección; PU = personal usuario; RI = responsable del área de informática; PI = personal de informática; RAI = responsable del área de auditoría en informática; LP = líder del proyecto de auditoría en informática; AI = auditor en informática

ETAPA ADECUACION

Esta etapa se enfoca en el análisis, adecuación y actualización de todos los elementos que intervienen en un proyecto de auditoria informática.

Es un conjunto de tareas estructuradas básicamente para que el proyecto de auditoria en informática se adapte a las necesidades de la empresa estudiada. En este punto resulta, pues, de suma importancia recalcar que la metodología tratada no se limita a la auditoria en informática para grandes corporaciones o centros de cómputo de magnitudes considerables.

Al terminar la presente etapa, el auditor en informática tendrán el apoyo bien especificado y clasificado; en las etapas restantes solo se desarrolla e implementa lo definido en la etapa actual.

El orden de las tareas de la etapa de adecuación puede variar conforme la experiencia, recursos, tiempos y prioridades que tenga la función de auditoria informática, esta etapa es más un trabajo interno que tareas que involucren a usuarios o personal de informática.

ETAPA	TAREAS	PRODUCTOS	REPONSABLE	INVOLUCRADOS
ADECUACIÓN	1. Definir objetivos del proyecto	1.1. Objetivos y alcances del proyecto	LP	RAI
	2. Definir etapas del proyecto y su detalle	2.1. Etapas y sus tareas	AI / RAI	RAI
		2.2. Plan actualizado	AI	LP
		2.3. Responsables e involucrados	AI	LP
		2.4. Productos terminados	AI	LP
		2.5. Revisiones (formales e informales)	AI	LP
	3. Definir los elementos por auditar por área de revisión	3.1. Aspectos o elementos por evaluar por cada área de revisión	AI	LP
	4. Establecer técnicas y herramientas por área de revisión	4.1. Técnicas	AI	LP
		4.2. Software	AI	LP
		4.3. Equipo de cómputo	AI	LP
		4.4. Otros de interés para el auditor	AI	LP
	5. Definición o actualización de políticas por área	5.1. Políticas y procedimientos por verificar de acuerdo con cada área que será auditada	AI	LP
		5.2. Políticas complementarias	AI	LP
	6. Elaboración o actualización de cuestionarios por área	6.1. Cuestionarios para cada área que será auditada	AI	LP
		6.2. Cuestionarios adicionales	AI	LP

Nomenclatura: AD = alta dirección; PU = personal usuario; RI = responsable del área de informática; PI = personal de informática; RAI = responsable del área de auditoría en informática; LP = líder del proyecto de auditoría en informática; AI = auditor en informática

ETAPA DE FORMALIZACIÓN

Las fases anteriores fueron de introducción e investigación del negocio y sus diversas funciones; y en ellas se detectaron las debilidades y fortalezas más relevantes en donde se define la planeación y la proyección de las áreas que requieren ser revisadas, y se documentan las adecuaciones o agregados requeridos. En esta etapa (formalización) que corresponde a la alta dirección dar su aprobación y el apoyo formal para el para el desarrollo del proyecto presentado por el líder del proyecto y el responsable de la función de dicha auditoria.

El objetivo primarios es justificar el desarrollo del proyecto en base a todos los argumentos y detalles encontrados, analizados y clasificados en fases anteriores y la duración de dicha etapa no debe ser muy prolongada puesto que ya se obtuvo la aprobación de usuarios clave y personal de informática en la etapa de adecuación, conviene tener en cuenta que la etapa de formalización se puede desarrollar al mismo tiempo que la etapa de adecuación si existen los recursos y el personal se encuentra disponible.

ETAPA	TAREAS	PRODUCTOS	REPONSABLE	INVOLUCRADOS
FORMALIZACIÓN	1. Verificar prioridades y cursos de acción	1.1. Prioridades clasificadas	LP	RAI
		1.2. Áreas por auditar verificadas	AI / LP	RAI
	2. Verificar plan y actividades	2.1. Etapas y sus tareas		
		2.2. Plan detallado final	AI	LP / AI
	3. Presentación formal del proyecto	3.1. Proyecto revisado de la auditoría	RAI	AD / PU / RI
	4. Aprobación formal del proyecto de auditoría en informática	4.1. Aprobación del proyecto	AD / PU / RI	RAI / LP
		4.2. Compromiso ejecutivo	AD	RAI / RI /PU
		4.3. Inicio formal del proyecto	LP	AD / PU / PI
	5. Presentación del proyecto a los usuarios de informática	5.1. Entendimiento del proyecto	RI	LP / AI
		5.2. Aceptación del proyecto	PI / PU	LP / AI
		5.3. Compromiso de cada una de las áreas involucradas	PI / PU	LP / AI
	6. Definir las áreas por visitar y concertar citas con el personal que se va a entrevistar	6.1. Fechas de entrevistas	LP	PI / PU
		6.2. Fechas de visitas	LP	PI / PU
		6.3. Fechas para aplicación de cuestionarios	LP	PI / PU

Nomenclatura: AD = alta dirección; PU = personal usuario; RI = responsable del área de informática; PI = personal de informática; RAI = responsable del área de auditoría en informática; LP = líder del proyecto de auditoría en informática; AI = auditor en informática

ETAPA DE DESARROLLO

Una vez hecho el diagnostico de donde se desprenden de donde se desprenden los riesgos y debilidades más importantes de los diferentes componentes relacionados con informática y elaborados y aprobados la matriz de riesgos y el plan de auditoria en informática, se realiza la auditoria en informática de cada área.

Es importante recordar que las etapas previas fueron de recopilación, análisis y diagnóstico de todas las áreas de informática de la empresa. En la etapa de desarrollo se revisan las áreas mencionadas en la matriz de riesgos y aprobada en el plan de trabajo acordado.

En esta etapa, la aplicación de los conocimientos y experiencia de los auditores da resultados que salvaguardan la integridad y rentabilidad de la información y de otros recursos de informática de la empresa.

ETAPA	TAREAS	PRODUCTOS	REPONSABLE	INVOLUCRADOS
DESARROLLO	1. Concertar citas	1.1. Fechas aprobadas o actualizadas	AI	PI / PU
	2. Verificar tarea, involucrados, etc.	2.1. Tareas, involucrados, etc. Revisados	AI	PI / PU
	3. Clasificar técnicas, cuestionarios y herramientas por usar	3.1. Técnicas clasificadas	AI	LP
		3.2. Cuestionarios clasificados	AI	LP
		3.3. Herramientas clasificadas	AI	LP
	4. Efectuar entrevistas	4.1. Entrevistas realizadas	AI	PI / PU
		4.2. Entrevistas documentadas	AI	AI
		4.3. Análisis de entrevistas	LP / AI	RAI
	5. Aplicar cuestionarios	5.1. Cuestionarios aplicados	AI	PI / PU
		5.2. Cuestionarios documentados	AI	AI
		5.3. Análisis de cuestionarios	LP / AI	RAI
	6. Efectuar visitas de verificación	6.1. Visitas realizadas	AI	RI / PI / PU
		6.2. Comentarios documentados	AI	AI
		6.3. Análisis de comentarios	LP / AI	RAI

7. Elaborar informe preliminar acerca de las áreas auditadas	7.1. Observaciones (acerca de debilidades o carencia de controles	AI	LP
	7.2. Áreas de oportunidad	AI	LP
	7.3. Alternativas por cada área de oportunidad detectada	AI	LP
	7.4. Recomendaciones (acciones específicas) por alternativa	AI	LP
	7.5. Responsables de ejecutar cada acción	AI	LP
	7.6. Plazos de ejecución por acción	AI	LP
	7.7. Áreas auditadas clasificados	AI	LP
	7.8. Informe documentado, almacenado y clasificado	AI	AI
8. Revisar el informe preliminar por área	8.1. Borrador de auditoría en informática revisado	LP	RAI / AI
9. Autorizar el borrador del informe preliminar	9.1. Informe preliminar revisado	LP	PI / PU / AI
	9.2. Informe preliminar corregido	AI	LP
	9.3. Informe preliminar entregado	LP	LP
	9.4. Informe preliminar autorizado	AD / PI / PU	AD / PI / PU

10. Efectuar entrevistas, cuestionarios y visitas complementarias	10.1. Entrevistas, cuestionarios y visitas pendientes realizados	LP / AI	PI / PU
	10.2. Informe actualizado con observaciones, acciones, etc.	AI	LP
11. Elaborar informe final	11.1. Informe final revisado con información de todas las áreas auditadas	AI	LP
	11.2. Informe con visto bueno del responsable de la función de auditoría en informática	RAI	LP / AI
	11.3. Informe final almacenado en medios magnéticos (respaldo)	AI	AI
	11.4. Documentación del informe para la alta dirección	LP / AI	RAI
	11.5. Documentación del informe para responsables de los usuarios de informática e informática	AI	LP
12. Elaborar un plan de implantación general de acciones sugeridas	12.1. Acciones clasificadas por plazos sugeridos	LP / AI	RAI
	12.2. Costo / beneficio del plan	LP / AI	RAI
13. Aprobar informe y plan de implantación	13.1. Informe de auditoría en informática y plan aprobados	AD / RI / PU	RAI / LP

14. Presentación del informe de auditoría en informática y del plan de implantación	14.1. Informe final y plan presentados a la dirección	RAI	AD / PI / LP
	14.2. Informe final y plan presentados a personal usuario y de informática	LP / AI	PI / PU
15. Aprobar informe final	15.1. Revisión del informe de auditoría en informática	AD / RI / PU	RAI / LP / PI
	15.2. Aprobación del informe de auditoría en informática	AD / RI	RAI / LP / PU
	15.3. Compromiso ejecutivo	AD / RI	RAI / PU

Nomenclatura: AD = alta dirección; PU = personal usuario; RI = responsable del área de informática; PI = personal de informática; RAI = responsable del área de auditoría en informática; LP = líder del proyecto de auditoría en informática; AI = auditor en informática

ETAPA DE IMPLANTACIÓN

Esta etapa determinante abarca:

- Definición de requerimientos para el éxito de la etapa de implantación.
- Desarrollo del plan de implantación.
- Implantación de las acciones sugeridas por la auditoria en informática.
- Seguimiento de la implantación.

Una vez que se revisan las áreas correspondientes y tanto los usuarios como el responsable de informática aprueban formalmente el plan de implantación, se establecen las políticas, procedimientos y estándares para cada recomendación del informe emanada de la etapa de desarrollo.

Elementos clave de la etapa de implantación son, entre otros:

- Ejecutar las acciones en los tiempos definidos en el plan de implantación.
- Asignar los usuarios o el personal de informática responsables de la implantación.
- Apoyo de la alta dirección para que actúen como facilidades de la implantación.
- Seguimiento formal y oportuno de la implantación por parte de los auditores en informática.
- Diferenciar y clasificar las acciones inmediatas, a corto o mediano plazo.
- Brindar los recursos necesarios para la terminación exitosa de la presenta etapa.

Algunas recomendaciones para llevar a buen término dicha revisión son las siguientes:

Estructurar un plan de visitas rápidas a las áreas más importantes de la función de informática que se evaluaron, para tomar las medidas necesarias que aseguren la correcta implantación de estándares, políticas o procedimientos relativos e informática.

ETAPA	TAREAS	PRODUCTOS	REPONSABLE	INVOLUCRADOS
IMPLANTACIÓN	1. Definir requerimientos para el éxito del plan de implantación	1.1. Recursos requeridos para el éxito de la implantación sugerida por la auditoría en informática	RI / PU	LP
		1.2. Recursos aprobados	AD	RI / PU / LP
		1.3. Equipo de trabajo para la implantación	RI / PU	LP
		1.4. Equipo de trabajo aprobado	AD	RI /PU /LP
		1.5. Funciones y responsabilidades	RI / PU	LP
		1.6. Fechas de revisión	RI / PU	LP
		1.7. Productos terminados	RI / PU	LP
		1.8. Costo / beneficio revisado	RI / PU	LP
		1.9. Costo / beneficio aprobado	AD	RI /PU /LP
		1.10. Inicio de la implantación	RI / PU	LP
	2. Desarrollar el plan de implantación detallado	2.1. Plan de implantación revisado según los resultados de la primera tarea	RI / PU	LP / AI
		2.2. Plan de implantación corregido y actualizado	PI	AI / PU
		2.3. Documentar plan final	RI	AI / PU
		2.4. Plan final aprobado	AD	PI / PU / LP
	3. Efectuar implantación sugerida por auditoría en informática	3.1. Inicio del proyecto	PI / PU	RI
		3.2. Tareas terminadas	PI / PU	RI
		3.3. Pendientes justificados	PI / PU	AD / RI
		3.4. Pendientes implantados	PI / PU	RI
		3.5. Presentación de implantación	RI	AD / RAI / LP
		3.6. Implantación aprobada	AD / PI / PU	RI / RAI / LP
	4. Seguimiento a la implantación del plan recomendado para la auditoría	4.1. Acciones de seguimiento seleccionadas	LP	RAI / AI
		4.2. Seguimiento de la implantación	LP	AI

	4.3. Revisiones informales	LP	AI
	4.4. Revisiones formales	LP	RAI
	4.5. Aseguramiento de calidad	LP	RAI
	4.6. Pendientes revisados	LP	RAI
	4.7. Pendientes aprobados	LP	RAI
	4.8. Seguimiento de pendientes	LP	RAI
	4.9. Implantación exitosa final	LP	RAI
	4.10. Implantación aprobada	RAI	RAI

Nomenclatura: AD = alta dirección; PU = personal usuario; RI = responsable del área de informática; PI = personal de informática; RAI = responsable del área de auditoría en informática; LP = líder del proyecto de auditoría en informática; AI = auditor en informática

Con lo anterior se sientan las básicas y principales bases del Sistema de Gestión de Seguridad de la Información para entender como está como está conformado que normas y estándares lo rigen y bajo que principios trabaja, entrando así de lleno en esta materia a continuación en donde se planteara un prototipo de proyecto, su desarrollo, sus resultados y soluciones.

C A P I T U L O 2

PROCESO DE DISEÑO E IMPLEMENTACION DEL SGSI

En este capítulo se presenta una propuesta de proyecto de implementación del Sistema de Gestión de Seguridad de la Información “SGSI” el cual está alineado con el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones “MAAGTIC” y por ser un organismo del ramo gubernamental en donde se aplicara dicha propuesta de proyecto es obligatorio apegarse a este estándar, a continuación hago un breve semblanza de lo que es este estándar.

¿Qué es MAAGTIC?

El MAAGTIC es una normatividad para la eficiencia operativa gubernamental de las operaciones del área de Tecnologías de la Información y Comunicación emitido por la Secretaría de Función Pública el 13 de julio de 2010 publicado en el Diario Oficial de la Federación (DOF) en la que se establece el acuerdo por el que se expide el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones (MAAGTIC)

¿QUE CONTIENE EL MAAGTIC?

El MAAGTIC contiene las reglas, acciones y procesos que en materia de Tecnologías de la Información y Comunicaciones (TIC) deberán observar de manera obligatoria, las dependencias y entidades de la Administración Pública Federal en México y, cuando corresponda, a la Procuraduría General de la República.
El MAAGTIC establece un marco rector de procesos, fundamentados en las mejores prácticas de TIC.

ALCANCE DEL MAAGTIC

El MAAGTIC está compuesto por 30 procesos, que se integran en 11 grupos, los cuales a su vez están considerados en 4 niveles de gestión, que conforman el “Marco rector de procesos de las TIC’s”.

Proceso en Materia de TIC (Tecnologías de la Información y Comunicaciones):

¿Y CUAL ES EL RETO DE LAS EMPRESAS QUE PRESTAN SERVICIOS AL GOBIERNO Y ESTAR ALINEADOS CON EL MAAGTIC?

Tener muy en claro el tipo de proyecto para definir y poner en marcha el marco rector de procesos en cumplimiento con lo dispuesto en el MAAGTIC, considerando para ello el escenario actual de la organización (entidad de gobierno), donde se pueden enfrentar situaciones como son:

- Restricción presupuestal
- Recursos humanos limitados
- Procesos desarrollados por terceros
- Necesidad de éxitos rápidos con resultados visibles en la implementación

PERO DE QUE DEPENDE EL ÉXITO PARA LOGRAR EL ALINEAMIENTO CON EL MAAGTIC

1. Evaluar la madurez actual de la UTIC (unidad administrativa de la Institución responsable de proveer de infraestructura y servicios de TIC a las demás áreas y unidades administrativas de la Institución) en lo que se refiere a los procesos, gente y tecnología
2. Identificar los procesos que conformarán el marco rector de procesos de la UTIC y conformar el plan de trabajo
3. Definir los procesos, políticas y controles internos que conformarán el marco rector de procesos
4. Poner en marcha los procesos que conforman el marco rector de procesos
5. Monitorear, mantener y mejorar el marco rector de procesos

Principales actividades para el alineamiento con el MAAGTIC
Esta son solo algunas de las actividades importantes para el alineamiento de cada proceso

Procesos	Gente	Tecnología
Identificación de procesos y prácticas adoptadas Mapeo de procesos Análisis de Brechas Elaboración de propuestas de diseño de procesos Desarrollo de políticas, procedimientos e indicadores Definición de roles y responsabilidades Documentación. Establecimiento de Controles Auditorías	Desarrollo de los Medios de Comunicación Capacitación en los procesos Capacitación en las mejores prácticas Definición de estrategias Desarrollo y diagnóstico de la comunicación	Definición para el establecimiento de controles basados en TI Identificación de soluciones tecnológicas Evaluación de soluciones tecnológicas para automatizar procesos Implementación, configuración y puesta a punto de las soluciones tecnológicas Configuración y ejecución de las herramientas que soportarán los procesos

De forma general estas serías las actividades y pasos a seguir de toda empresa y/0 gobierno que se encuentra en alineamiento con el MAAGTIC.

PRESENTACION DEL PROYECTO

PROYECTO PRESENTADO POR LA EMPRESA *CONSULTOR REVISOR DEL SGSI* PARA EL *ORGANISMO RECEPTOR* PARA REVISAR, IMPLANTAR Y/O MODIFICAR EL SGSI EN LA DEPENDENCIA.

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION CON BASE EN MAAGTIC.

1. INTRODUCCIÓN

En el ***ORGANISMO RECEPTOR DEL SERVICIO*** se requiere proporcionar los mecanismos y procedimientos para la administración, gestión de la seguridad de la información **para garantizar la infraestructura de seguridad de información en el área de TIC**.
En este documento se describe la propuesta de servicios de mantenimiento para el Sistema de Gestión de Seguridad de Información de ***ORGANISMO RECEPTOR DEL SERVICIO*** por parte del ***CONSULTOR REVISOR DEL SGSI***, con base en el MAAGTIC y con apoyo de estándares internacionales como lo es ISO 27001 e ISO 27005.

2. METODOLOGÍA

A continuación se muestra la metodología para la **implementación** de procesos de seguridad de información, utilizada por el ***CONSULTOR REVISOR DEL SGSI***.

La metodología se divide en 5 fases que se describen a continuación, en donde cada una de ellas toma como punto común la transferencia de conocimiento al cliente.

FASE I.- EVALUACIÓN
FASE II.- ESTRATEGIA
FASE III.- IMPLANTACIÓN
FASE IV.- VERIFICACIÓN
FASE V.- MANTENIMIENTO/MEJORA

Fase I – Evaluación.- Esta fase comprende el reconocimiento del estado de la seguridad de la información en el ***ORGANISMO RECEPTOR DEL SERVICIO***, dando como resultado el estado de la práctica de seguridad de información en la organización para dar pie a la creación y/o recomendación de la Política de Seguridad de Información y Políticas de Protección de Información requeridas para fundamentar el Sistema de Gestión de Seguridad de Información *(SGSI)* del ***ORGANISMO RECEPTOR DEL SERVICIO***.

En esta fase se cubre la etapa del **PLAN** del modelo de mejora continua de Deming requerido por MAAGTIC en el "OSGP-1 Implementar el Sistema de Gestión y Mejora de los Procesos de la UTIC" del proceso "5.4.1 Operación del Sistema de Gestión y Mejora de los procesos de la UTIC".
Fase II – Estrategia.- En esta fase se definen los controles del SGSI con base en requerimientos legales, compromisos contractuales y regulatorios a los que está obligado el ***ORGANISMO RECEPTOR DEL SERVICIO*** a cumplir. Esta fase da como resultado un plan de acción detalladlo a ser implementado en las diferentes áreas del ***ORGANISMO RECEPTOR DEL SERVICIO*** involucradas en el alcance del SGSI.

Fase III – Implementación.- Esta fase es en donde se implementa el SGSI conforme a la estrategia planteada en la fase anterior y se madura la operación del proceso por al menos 3 meses, que son requeridos para poder ser candidatos a la certificación MAAGTIC.

En esta fase se cubre la etapa de **DO** del modelo de mejora continua de Deming requerido por MAAGTIC en el "OSGP-2 Ejecutar la Planeación de Implementación de Mejora de los Procesos y Operar el Sistema de Gestión y Mejora de los Procesos de la UTIC." Del proceso "5.4.1 Operación del Sistema de Gestión y Mejora de los Procesos de la UTIC".

Fase IV – Verificación.- En esta etapa se monitorean los resultados del SGSI y se audita de forma interna al SGSI dentro de su alcance con base en el estándar MAAGTIC.

En esta fase se cubre la etapa de **CHECK** del modelo de mejora continua de Deming requerido por MAAGTIC, en el "OSGP-3 Monitorear y Evaluar la Operación del Sistema de Gestión y Mejora de los procesos de la UTIC" del proceso "5.4.1 Operación del Sistema de Gestión y Mejora de los Procesos de la UTIC".

Fase V – Mantenimiento, Mejora.- En esta fase se revisan los resultados del SGSI con base en los resultados de las etapas anteriores del modelo Deming (PLAN, DO, CHECK) y se generan acciones de mejora continua.

En esta fase se cubre la etapa de **ACT** del modelo de mejora continua de Deming requerido por MAAGTIC, en el "OSGP-4 Ejecutar la Acciones de Mejora a los Procesos de la UTIC" del proceso "5.4.1 Operación del Sistema de Gestión y Mejora de los Procesos de la UTIC".

Como se ha definido en las fases descritas, esta metodología de implementación sigue el modelo de mejora continua de Deming **PLAN, DO, CHECK** y **ACT**, requerido por el estándar MAAGTIC, en el proceso "**5.4.1 Operación del Sistema de Gestión y Mejora de los Procesos de la UTIC**" (***ANEXO A***), como parte del alcance de esta propuesta se definirá el ciclo de vida para el Sistema de Gestión de Seguridad de Información requerido en el proceso "**5.9.4 Administración de la Seguridad de Información**" (***ANEXO B***) con apoyo del manejo de riesgos "**5.2.2 Administración**

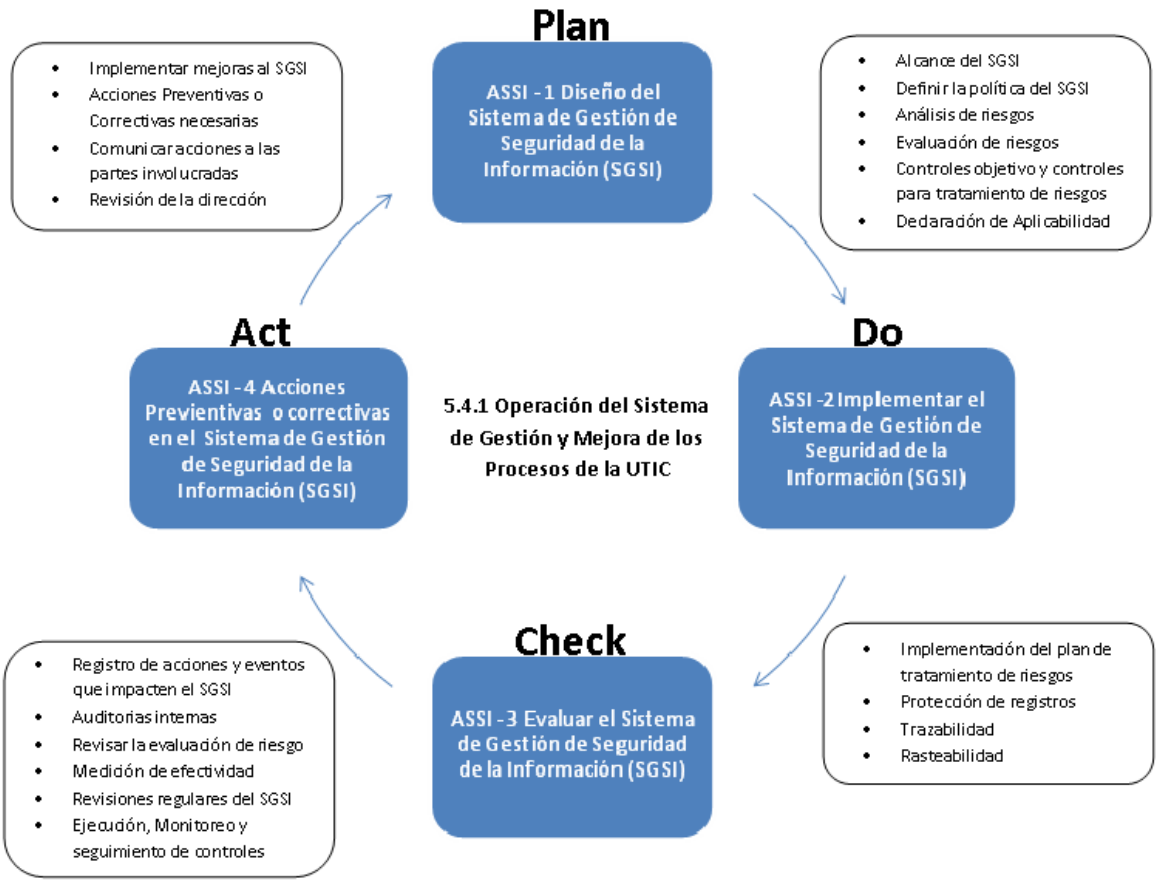
de Riesgos" (***ANEXO C***) y la definición de indicadores requeridos en el proceso "**5.2.1 Administración de la evaluación de TIC**" (***ANEXO D***).

Para la definición, desarrollo, puesta en operación y evaluación del SGSI, se utilizará el ciclo PDCA (Plan-Do-Check-Act), con base en el modelo de mejora continua de Deming como lo requiere el proceso "5.4.1 Operación del Sistema de Gestión y Mejora de los Procesos de la UTIC".

3. ALCANCES

El alcance de esta propuesta es para el desarrollo de un Sistema de Gestión de Seguridad de información para el ***ORGANISMO RECEPTOR DEL SERVICIO*** que englobará las fases de la metodología mencionada anteriormente.

FASE I.- EVALUACIÓN
FASE II.- ESTRATEGIA
FASE III.- IMPLANTACIÓN
FASE IV.- VERIFICACIÓN
FASE V.- MANTENIMIENTO/MEJORA



Durante el desarrollo del sistema de Gestión de seguridad de información del ***ORGANISMO RECEPTOR DEL SERVICIO*** se incluyen entregables en cada fase de la metodología de implantación como se detalla en esta propuesta.

3.1. Fase I – Evaluación

Durante esta fase se realiza un **Análisis de Riesgos con base en los requisitos del proceso "5.2.2. Administración de riesgos de TIC"** del MAAGTIC donde se obtiene el estado de la práctica de la seguridad de información del ***ORGANISMO RECEPTOR DEL SERVICIO*** **en el alcance definido para el SGSI**.

Se debe tomar en cuenta las siguientes actividades a desarrollar o apoyar en esta fase para solventar los requerimientos de la etapa del **PLAN** del modelo de mejora continua de Deming solicitado por MAAGTIC:

- **Definir y validar el alcance del SGSI** en términos de las características de los Procesos de Negocio y Procesos de Soporte de la organización, localización, activos de información, e infraestructura tecnológica, leyes, regulación, incluyendo detalles y justificación de cualquier exclusión, contratos, convenios y características de operación de procesos.
- **Definir la política del SGSI** en términos del alcance definido, como de la organización, ubicación, activos, tecnología, leyes, regulaciones, contratos, convenios y características de operación de procesos de negocio.

  Se considera en la política un marco de trabajo, objetivos, dirección y principios para acciones de la seguridad de información y todo aquello que requiera de acuerdo a los controles del MAAGTIC. Lo anterior se toma del PROCESO 5.9.4 ASSI, 5.9.4.4 REGLAS DE OPERACIÓN, 1.6 REGLAS MINIMAS QUE DEBERAN SER OBSERVADAS POR LAS UTIC, RELACIONADAS CON LA SEGURIDAD DE LA INFORMACIÓN CONTENIDA EN MEDIOS ELECTRÓNICOS, requeridos por la organización que establece**:**

  General:
  Establecer los mecanismos que permitan la administración de la seguridad de la información de la Institución contenida en medios electrónicos y sistemas informáticos.

  Específicos:
  1. Establecer un Sistema de Gestión de Seguridad de la Información (SGSI) que proteja la información de la Institución contenida en medios electrónicos y sistemas informáticos, contra accesos y usos no autorizados, con la finalidad de conservar su confidencialidad, integridad y disponibilidad.

  5.9.4.4 en su punto 1.6 dice lo siguiente:

  1.6 Las reglas mínimas que deberán ser observadas por la UTIC, relacionadas con la seguridad de la información contenida en medios electrónicos, se encuentran disponibles en la página **www.maagtic.gob.mx**

Anexo al proceso:

5.9.4	**ASSI**	**Administración de la Seguridad de la información**
5.9.4.4		**Reglas de Operación**
1.6		**Reglas mínimas que deberán ser observadas por las UTIC, relacionadas con la seguridad de la información, ordenadas por Objetivo de Control según el marco ISO 27001**

A.5 Política de Seguridad

1. Todo el personal de la dependencia o entidad está obligado a operar en un ambiente de trabajo que garantice la confidencialidad, integridad y disponibilidad de la información, de acuerdo a las disposiciones de la presente norma.

2. Las reglas de operación de los procedimientos de seguridad de la información, deberán revisarse y actualizarse cuando cambien las condiciones de las soluciones tecnológicas o cuando cambie la legislación aplicable.

A.6 Organización de la Seguridad de la información

1. El personal de la UTIC responsable de la seguridad de los recursos de TIC deberá certificar que el personal externo, que tenga cualquier tipo de contacto con recursos de TIC institucionales cumpla con las disposiciones de este manual.

2. Las instituciones no otorgarán el derecho de intercambio de información con entidades externas en caso de que los controles identificados por al UTIC en estas últimas no cumplan satisfactoriamente con la información de la dependencia o entidad.

3. Se permitirá al personal de los proveedores de servicios el acceso a los puntos de red únicamente con la autorización del responsable del proyecto o proceso en el que trabaje ese personal.

4. El personal de la UTIC con atribuciones para ello será responsable de autorizar los accesos del personal de los proveedores de servicios y del registro correspondiente.

A.7 Administración de Activos

1. Los propietarios de la información son los responsables de la custodia y buen uso de la información que se almacena, procesa y transmite dentro de las instituciones.

2. Los usuarios de TIC y, en particular los propietarios de la información almacenada en medios electrónicos, definirán los requerimientos de seguridad de su información y de sus sistemas de información.

3. La UTIC, en conjunto con los usuarios responsables de la información clasificada como confidencial o reservada, determinará los esquemas de seguridad que se aplicarán para mantener su confidencialidad, disponibilidad e integridad.

4. La información clasificada según la LFTAIPG (Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental) como confidencial o reservada deberá residir en territorio nacional. Los servicios de almacenamiento y administración de la misma deberán realizarse de igual manera dentro del territorio nacional.

5. Las UTIC y sus usuarios deberán apegarse al esquema de la APF (Administración Pública Federal) para la clasificación de la información, a fin de definir sus niveles de protección.

6. La información que se genera, almacena, procesa y transmite por medios electrónicos será almacenada, resguardada y administrada por la UTIC en función de la clasificación indicada por los usuarios propietarios o responsables de ella, al momento de definir los requerimientos de las soluciones tecnológicas o servicios de TIC que se construyan para cada usuario.

7. Las UTIC y los usuarios involucrados deberán velar por que cada medio de almacenamiento desmontable o removible, con información clasificada como confidencial, reservada o pública, sea etiquetado por el responsable del mismo, de acuerdo a la normatividad vigente.

8. La UTIC, en conjunto con los usuarios de la información almacenada en medios electrónicos clasificada como confidencial o reservada, determinarán los esquemas de seguridad necesarios para mantener su confidencialidad, disponibilidad e integridad.

A.8 Seguridad de los Recursos Humanos

1. El usuario debe de dar cumplimiento a todas las disposiciones que le sean comunicadas por UTIC, tanto relacionadas con el uso de las soluciones tecnológicas, los servicios de tecnologías de la información, como equipos PC. Debe también estar al tanto de sus responsabilidades, por lo que debe firmar, bajo protesta de decir verdad, que conoce las disposiciones, el inventario de software y hardware instalado en su equipo.

2. Las UTIC deberán fijar los mecanismos de seguridad de la información para el personal en aquellos cargos de la estructura organizacional de la UTIC donde se maneje información confidencial.

A.9 Seguridad Física y Ambiental

1. La UTIC deberá implementar mecanismos de control de acceso a las instalaciones del centro de datos, del centro de telecomunicaciones y de todas aquellas instalaciones en las que se encuentre equipo de almacenamiento, procesamiento y/o transmisión de información. La UTIC debe contar con mecanismos de control que permitan asegurar que el personal que ingrese a sus instalaciones cuente con la autorización correspondiente.

2. El personal de la UTIC que administre la infraestructura de TIC debe llevar un registro del personal y justificar el motivo de acceso a las áreas en las que se encuentran estos componentes. El registro que ingreso a las áreas citadas.

3. El personal de la UTIC que administre la infraestructura de TIC debe mantener actualizadas a las listas de autorización de acceso a personal de proveedores de servicios

de terceros y llevar el control de accesos presenciales y remotos indicados en el punto anterior.

4. Se permitirá el personal de los proveedores de servicios el acceso a los puntos de red incluyendo el acceso a los nodos de la red de la dependencia o entidad solo bajo la supervisión de las instalaciones físicas de TIC. El personal de los proveedores de servicios deberá presentar identificación oficial y de la empresa que representa al momento de solicitar el acceso.

5. El personal de la UTIC debe instalar la infraestructura de TIC en ambientes físicos adecuados para su operación, administración, monitoreo y control de acceso, para minimizar los riesgos, amenazas, y condiciones de operación fuera de las especificaciones indicadas por los proveedores correspondientes.

6. Los usuarios de equipos de cómputo de escritorio deben asegurarse de utilizar y mantener cerradas las chapas de seguridad de estos equipos. Los usuarios de equipos de portátiles deberán asegurarse de colocar el cable y candado de seguridad correspondiente.

7. Vía la mesa de servicios, el personal de la UTIC responsable de la seguridad de los recursos de TIC, se asegurará de que el equipo de escritorio, portátil, o de cualquier otro tipo, que utiliza la conexión a la red institucional se encuentre libre de virus informático.

8. La UTIC, siguiendo el proceso de Administración de la infraestructura física de TIC, deberá evaluar y certificar la seguridad de las instalaciones eléctricas, de comunicaciones, de sistemas contra incendios, de aire acondicionado y de otros recursos, que garanticen las condiciones adecuadas de seguridad para la operación de la infraestructura física de TIC de la dependencia o entidad.

9. Las UTIC deberán asegurar que los nodos de comunicaciones a las redes institucionales estén ubicados en lugares cerrados y resguardados.

A.10 Gestión de las Comunicaciones y Operaciones

1. Vía la mesa de servicios, el personal responsable de la seguridad de los recursos de TIC se asegurará de que el equipo que utilizará la conexión a red institucional se encuentre libre de virus informáticos, así como lo necesario para mantener su seguridad y la de la red institucional.

2. Los usuarios y el área de soporte técnico de la UTIC de forma periódica (semestral, mensual, quincenal) deben realizar copias de seguridad de la información crítica que almacenen en su equipo.

3. La UTIC deberá solicitar a los usuarios responsables de los servicios, las necesidades del respaldo de sus datos. Estos deberán tomar en cuenta el tipo de información y las necesidades de operación de los propios servicios, en apego a la normatividad aplicable.

   El área de la UTIC designada responsable de la ejecución de los respaldos deberá efectuarlos en estricto apego a los requerimientos indicados por los usuarios.

4. El área de la UTIC designada responsable deberá elaborar el calendario de respaldos y comunicarlo a la UTIC, considerando las necesidades de los usuarios responsables de los servicios, así como las necesidades de las soluciones tecnológicas y centro de datos del al UTIC

5. El área de la UTIC desinada responsable del calendario de respaldos deberá conservar evidencia del respaldo efectuado y garantizar la integridad de la información

6. El área de la ITIC designada responsable deberá mantener los controles necesarios para conocer el estado de cada copia de respaldo y ubicación.

7. El área de la UTIC designada responsable deberá implantar procedimientos para preparar y almacenar la información y probar periódicamente la integridad de los respaldos.

8. El área de la UTIC designada responsable deberá mantener una copia del software, soluciones tecnológicas, aplicativos, parámetros de configuración de ambientes, estructuras de datos t datos; anterior a la versión en operación.

9. El área de la UTIC designada responsable deberá generar las copias necesarias de los respaldos y almacenarlas en inmuebles diferentes, a fin de garantizar la recuperación de la operación, en caso de ejecutarse algún plan de contingencia.

10. El área de la UTIC designada responsable deberá registrar en una bitácora de evidencias las repercusiones realizadas, indicando al menos, el número de solicitud de la restauración, el dueño de la información, el nombre del sistema, la sección solicitada y el número de serie del respaldo utilizado.

11. El área de la UTIC designada responsable deberá atender solamente las solicitudes de restauración efectuado por escrito; la solicitud deberá contener al menos: nombre del propietario de la información, nombre del sistema del cual se desea recuperar la información, especificaciones de la información que se desea recuperar.

12. El área de la UTIC designada responsable en conjunto con las áreas propietarias de la información y/o las soluciones tecnológicas determinará la permanencia y la vigencia de la información respaldada, en concordancia con la legislación aplicable.

13. El área de la UTIC designada responsable deberá en conjunto con las áreas propietarias de la información, definir el mecanismo especifico, por sistema o por tipo de información, de eliminación de respaldos.

14. Los usuarios que requieran conectarse a la red institucional utilizando equipo de cómputo de escritorio o portátil, propio o institucional, deberán obtener autorización de la UTIC vía la mesa de servicios, la cual será responsable de habilitar su conexión.

15. La información confidencial o reservada contenida en medios de almacenamiento bajo responsabilidad de la UTIC que vayan a dejar de usarse, deberán ser borrados mediante un medio que garantice la eliminación física total de la información. Deberá aplicarse también se van a ser utilizados o entregados a un tercero para reparación o en préstamo.

Deberá obtenerse una evidencia de la eliminación. Si los medios de almacenamiento de los equipos y accesorios están bajo el resguardo de los usuarios, estas acciones serán responsabilidad del usuario. En caso de requerirlo, podrán solicitar apoyo a la UTIC vía la mesa de servicios y apegarse a la normatividad aplicable.

16. El personal de la UTIC que administre la infraestructura de TIC debe evitar el acceso a los respaldos en los medios físicos de información, de personal no autorizado.

17. Las UTIC deben asegurarse de implementar bitácoras de seguridad en las que queden registrados por cuentas con permisos especiales, al menos: las de administrador, visitante, raíz y de sistema.

18. La UTIC deberá implementar un mecanismo de seguridad para que la bitácora electrónica de auditoría solo pueda ser consultada por cuenta de administración del responsable de seguridad del elemento de TIC considerado.

19. La UTIC debe definir e instrumentar un mecanismo de seguridad para evitar intrusiones a la infraestructura de TIC, incluyendo ataques externos vía internet, extranet e inclusive intranet.

20. La UTIC debe implementar un mecanismo para mantener informada de las actualizaciones de seguridad del software utilizado en la dependencia o entidad, de la aparición de nuevos virus informáticos que puedan atacar las soluciones tecnológicas y los equipos de los usuarios de la dependencia o entidad.

21. La UTIC, al identificar la existencia de un virus informático no cubierto por los antivirus institucionales en operación, en servidores y en equipos de los usuarios, notificará a la mesa de servicios de manera que, a través de esta, se difundan las medidas necesarias a los usuarios y estos se protejan hasta que la UTIC corrija la intrusión del virus y lo elimine.

22. La UTIC deberá instrumentar mecanismos de administración de los equipos de proceso y de comunicaciones, que incluyan revisiones periódicas de las bitácoras de los elementos de la infraestructura de TIC, para identificar si se han presentado intentos de ataques o explotación de vulnerabilidades.

23. El área de la UTIC deberá habilitar el registro de los incidentes de seguridad relacionados con los accesos a las soluciones tecnológicas y a las actividades realizadas por los usuarios.

A.11 Control de Acceso

1. El personal de la UTIC que administre la infraestructura de TIC debe controlar el acceso presencial y remoto a los componentes de cada uno de los elementos de la infraestructura de TIC de la dependencia o entidad.

2. Las UTIC deberán implantar mecanismos de seguridad para acceder a los datos almacenados, que respeten los principios de identidad, responsabilidad y rastreabilidad de

los usuarios que los acceden, en función del nivel de exposición y revelación de los mismos.

3. Las UTIC deberán asegurar que las capacidades de los usuarios para acceder a datos están limitadas de acuerdo al perfil que corresponda a sus funciones, previa definición de las UR propietarias de los datos y de las soluciones tecnológicas que hacen uso de ellos.

4. Las UTIC son las encargadas de implementar los mecanismos de seguridad necesarios para la asignación de los permisos de acceso a los usuarios, determinados por las UR responsables de la información.

5. El personal de la UTIC, que administre la seguridad de la infraestructura de TIC debe instrumentar el registro de usuarios y la administración de la seguridad de las soluciones tecnológicas de información que son accedidos en forma local y/o remota a través de la red de comunicación.

6. El personal de la UTIC que administre la seguridad de la infraestructura de TIC debe instrumentar mecanismos para que se efectué la personalización de las cuentas para las actividades de administración de servidores, bases de datos, servicios, o sistemas institucionales, así como para el monitoreo de las actividades realizadas por los usuarios.

7. La UTIC deberá instrumentar un mecanismo de seguridad pata que, desde su creación, todo usuario tenga definido el ambiente de trabajo acorde a sus funciones; éste no deberá poder ser modificado por el usuario, sino a través de una solicitud a la mesa de servicios.

8. El área de la UTIC designada responsable de la asignación de cuentas de usuario y contraseñas deberá asegurar que un solo responsable asigne cuentas de usuario para cualquiera de los servicios y/o sistemas que operan dentro de la dependencia o entidad.

9. El área de la UTIC designada responsable de la asignación de cuentas de usuario y contraseñas indicara a los usuarios las características de las contraseñas.

10. El área de la UTIC designada responsable de la asignación de cuentas de usuario y contraseñas deberá identificar y autenticar claramente al usuario antes de asignarle una cuenta.

11. El área de la UTIC designada responsable de la asignación de cuentas de usuario y contraseñas deberá eliminar cualquier cuenta de usuario que haya cambiado de situación laboral o no labore más en la dependencia o entidad.

12. Las contraseñas no deben ser mostradas en pantalla mientras son tecleadas, ni deben viajar por la red sin ser cifradas.

13. El área de la UTIC designada responsable de la asignación de cuentas de usuario y contraseñas deberá facilitar a los usuarios del correo electrónico, el cambio de contraseña cuando éstos lo estimen conveniente, o de acuerdo en lo establecido en el lineamiento de cambio de contraseña por caducidad.

14. Los usuarios deben verificar que su equipo de cómputo tenga configurado el protector de pantalla con contraseña, con la finalidad de evitar el acceso no autorizado a su formación en caso de retiro temporal.

15. Los usuarios están obligados a considerar que las cuentas y contraseñas asignadas son personales e intransferibles. Las consecuencias jurídicas y/o administrativas de los actos ejecutados con las mismas son responsabilidad exclusiva del usuario dueño de la cuenta.

16. Los usuarios deben evitar la repetición de contraseñas al efectuar los cambios periódicos de las mismas.

17. Los usuarios deben cambiar su contraseña en caso de sospechar que alguien más la conoce.

18. Los usuarios deben evitar exponer o difundir su contraseña independientemente del medio en el cual sea almacenada.

19. En caso de utilizar hardware de seguridad, tales como generadores de contraseñas o tarjeta inteligente, los usuarios deben traerlos siempre consigo.

20. La UTIC facultará al personal técnico para asegurar que todos los equipos de cómputo de escritorio y portátiles que se puedan conectar a la red institucional de la dependencia o entidad cumplan con los siguientes controles de acceso: nombre de equipo que identifique al responsable del equipo y su ubicación, integración a un dominio, tener instalado el software de antivirus institucional; contar con la última versión y parche del sistema operativo liberado por el proveedor.

21. La UTIC deberá implementar un mecanismo de seguridad en todos los elementos de comunicaciones para que todos los intentos de conexión hacia la infraestructura de TIC que soporta las aplicaciones o servicios institucionales pasen a través de un “cortafuego” (conocido comúnmente por su traducción en inglés: firewall).

22. La UTIC deberá implementar in situ los mecanismos de seguridad necesarios para el área de producción, y en caso de accesos remotos, deberá instrumentar el uso de software de cifrado de canal.

23. La UTIC deberá implementar un mecanismo de control para proveer el servicio de acceso remoto a la red institucional, a las soluciones tecnológicas, a los servicios de red y colaboración, así como a la información. El acceso será otorgado únicamente a los funcionarios y a los proveedores que lo requieran.

24. La UTIC deberá definir e implementar las herramientas de detección de intrusos y protección a vulnerabilidad alineadas a la infraestructura de TIC, sistemas de información, necesidades de servicios de red y colaboración de la dependencia o entidad.

25. El personal de la UTIC que administre la seguridad de la infraestructura de TIC debe limitar el acceso a los servidores, a sus sistemas operativos, a las soluciones tecnológicas institucionales y a las bases de datos, mediante la identificación del usuario, a través de su

cuenta única y contraseña; la UTIC deberá llevar un control de perfil y privilegios de acceso por usuario.

26. La UTIC deberá implementar en las soluciones tecnológicas y servicios a los usuarios, mensajes de ingreso en los cuales se les advierta que: el sistema y/o servicio solo podrá ser utilizado por personal autorizado, que las actividades realizadas son monitoreadas y rastreables y que cualquier intento de ingreso no autorizado será sancionado.

27. El área de la UTIC responsable de la asignación de cuentas de usuario y contraseñas o en su defecto, las soluciones tecnológicas y aplicaciones, deberán bloquear el acceso a toda cuenta de usuario después de 3 intentos consecutivos fallidos de acceso a las soluciones tecnológicas o red.

28. El área de la UTIC responsable de la asignación de cuentas de usuario y contraseñas o en su defecto, las soluciones tecnológicas y aplicaciones designadas como sensibles o críticas, deberán restringir el número de sesiones por usuario.

29. El área de la UTIC responsable de la asignación de cuentas de usuario y contraseñas, o en su defecto las soluciones tecnológicas y aplicaciones designadas como sensibles o críticas, deberán bloquear cualquier cuenta de usuario que no se haya firmado en el sistema o la red después de 30 días.

A.12 Adquisición, Desarrollo y Mantenimiento de Información

1. La UTIC deberá asegurar que la información institucional que se transmitan a través de las redes internas o externas se encuentre cifrada, con independencia de la clasificación confidencial o reservada a la que se encuentre sujeta. Para el caso del almacenamiento de los datos de acuerdo a la clasificación de la información, las definiciones del Grupo de seguridad del SGSI y de los requerimientos que los usuarios definan para sus sistemas o servicios, la información será encriptada.

2. La UTIC deberá implementar un mecanismo de control para que todo el personal responsable o poseedor de manuales, procedimientos, guías e instructivos de operación (en medio electrónico o papel) de los equipos de cómputo, telecomunicaciones y sistemas, controle y reporte el acceso y uso de los mismos, bajo su estricta responsabilidad.

A.13 Gestión de Incidentes en la Seguridad de la Información

1. Los usuarios que presencien o sospechen actos citados en la disposición anterior deberán notificarlo por escrito a su inmediato superior y al responsable del área de seguridad de la información.

2. El siniestro, extravió o robo de equipo de cómputo y/o periféricos deben ser reportados de forma inmediata por el usuario afectado (aquel que tiene bajo su resguardo el equipo siniestrado) al área administrativa correspondiente, para que se realicen las gestiones pertinentes.

A.14 Cumplimiento

1. Los datos clasificados como confidenciales o reservados deberán tener fechas programadas de eliminación y deberá destruirse la identificación del medio y cualquier

marca de uso, en estricto apego a la normatividad vigente en la materia y asegurando conservar la evidencia correspondiente del apego a la regla.

2. La información confidencial o reservada no necesaria deberá ser destruida, los listados deberán ser triturados y los desechos empacados antes de deshacerse de ellos, en estricto apego a la normatividad vigente en la materia y asegurando conservar evidencia correspondiente del apego a la regla

3. En caso de inobservancia y, a fin de garantizar la integridad, confiabilidad y disponibilidad de la información de la información de las instituciones, el personal responsable de la seguridad de los recursos TIC tendrá la obligación de suspender de manera inmediata los servicios de TIC al o los usuarios que hubiesen infringido alguna de las disposiciones de las disposiciones del presente manual.

4. La UTIC deberá asegurarse de que cualquier intento para obtener acceso no autorizado a la infraestructura, a los servicios o a los datos, la revelación no autorizada de información, el procesamiento o transmisión de datos, los cambios a las características de los activos de TIC sin autorización, o cualquier otra actividad en materia de TIC, que afecte a los intereses de la dependencia o entidad, sean informados a las instancias facultadas, para promover las sanciones aplicables de acuerdo a la reglamentación y legislación vigente aplicable.

Con base a lo anterior y en términos del alcance del SGSI, se actualizará, dentro de la Política de Seguridad de Información del ***ORGANISMO RECEPTOR DEL SERVICIO***, el marco general y los objetivos de seguridad de la información del ***ORGANISMO RECEPTOR DEL SERVICIO***, considerando los requerimientos legales o contractuales relativos a la seguridad de la información, alineándolos con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI. Debiéndose obtener la aprobación de la Política de Seguridad de Información por parte del grupo directivo del ***ORGANISMO RECEPTOR DEL SERVICIO***.

- Se documenta la **metodología de análisis y evaluación** de riesgos de seguridad de la información, conforme al estándar MAAGTIC a fin de establecer los criterios y la metodología de evaluación del riesgo, alineada a la norma MAAGTIC, de donde se obtengan resultados comparables y reproducibles apropiados a los requerimientos del ***ORGANISMO RECEPTOR DEL SERVICIO*** y el SGSI, en donde se especifiquen los niveles de riesgo aceptables y los criterios de aceptación de estos.

- Se realiza la **identificación de riesgos** de los riesgos y propietarios de esos activos; las amenazas para los activos que podrían ser explotadas por las vulnerabilidades detectadas; los impactos en pérdida de confidencialidad, integridad y disponibilidad en los activos de información. Tomando en cuenta la identificación de riesgos de acuerdo con:

    - Los activos que están dentro del alcance del SGSI y a sus responsables directos.
    - La identificación de las amenazas e relación a los activos.
    - La identificación de las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.
    - La identificación de los impactos en la confidencialidad, integridad y disponibilidad de los activos.

- Se **Analizan y Evalúan los riesgos** identificados en el punto anterior que podrían resultar de la falla de la falla en la seguridad, tomando en cuenta las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad en los activos, de acuerdo con:

    - El impacto en el SENAICA por incidentes de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información.
    - La probabilidad de ocurrencia de in incidente de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados.
    - La estimación de los nivele de riesgo.
    - La determinación, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser minimizado.

- Se identifican y evalúan **opciones para el tratamiento de riesgos** y se proponen las acciones a realizar, tomando en cuenta los siguientes criterios para tratar el riesgo:

    - Aplicar controles adecuados.
    - Aceptar el riesgo, siempre y cuando cumpla con las políticas y criterios establecidos para la aceptación de los riesgos.
    - Evitar el riesgo (p.e. Mediante el cese de escenario de riesgo que lo originan).
    - Transferir el riesgo a terceros (p.e. aseguradoras o contratos de outsourcing).

- Se **seleccionan los controles** objetivo y controles: del **anexo E** que cumplan con los requerimientos identificados en el proceso de evaluación y tratamiento del riesgo y se justifica la selección o exclusión.

- Se consigue **la aprobación**, por parte del grupo directivo, tanto los riesgos residuales como la implantación y uso del SGSI.

- Se define la **Declaración de Aplicabilidad**, donde se documentará los objetivos de control, los controles seleccionados y las razones para su selección. También se documentará el fundamento de la exclusión de objetivos de control y de controles del estándar MAAGTIC. Tomando en cuenta:

    - Los objetivos de control y controles seleccionados y los motivos para su elección.
    - Los objetivos de control y controles que actualmente y están implantados.
    - Los objetivos de control y controles del Anexo D excluidos y los motivos para su exclusión. A fin de detectar posibles omisiones involuntarias.

Estos entregables se darán en los formatos siguientes que marca el MAAGTIC.

OSGP – 1 (Dirigido exclusivamente al SGSI)

- Anexo 8, Formato 9 “Documento de planeación de evaluación”

ARTI – 1

- Anexo 5, Formato 1 “Descripción de roles y responsables del Grupo de trabajo de riesgos de TIC”
- Anexo 5, Formato 2 “Directriz rectora del proceso de administración de riesgos de TIC”

ARTI – 2

- Anexo 5, Formato 3 “Matrices de riesgo de TIC”
- Repositorio de riesgo de TIC

ARTI – 3
- Anexo 5, Formato 4 “Declaraciones de aplicabilidad”
- Anexo 5, Formato 5 “Programas de mitigación de riesgos”
- Anexo 5, Formato 6 “Programas de contingencias”
- Repositorio de riesgos de TIC.

ASSI – 1
- Anexo 24 , Formato 1 “Sistema de Gestión de Seguridad de la Información”

3.2. Fase II – Estrategia

En esta fase se crean las especificaciones de necesidades de seguridad de información a ser implementadas en el ***ORGANISMO RECEPTOR DEL SERVICIO*** tomando en cuenta puntos de tecnología, físicos y de procedimientos de seguridad de información por medio de un análisis detallado de los requerimientos operativos, técnicos, normativos e informáticos del ***ORGANISMO RECEPTOR DEL SERVICIO*** a fin de definir el plan de tratamiento de riesgos que identifique las acciones, recursos respo0nsabilidades y prioridades en la administración de los riesgos de seguridad de la información.

Se representa un programa de implementación del SGSI en el ***ORGANISMO RECEPTOR DEL SERVICIO*** con base en el plan de tratamiento de riesgos.

Esta fase solventa los requerimientos de la etapa **DO** del modelo de mejora continua de Deming solicitado por la cláusula **4.2.2 a)** del MAAGTIC.

Los productos de esta fase son los siguientes:
ASSI – 1
- Anexo 24, Formato 2 “Programa de implantación del Sistema de Gestión de Seguridad de la Información”

3.3. Fase III – Implantación

Apoyar en la implantación del plan de riesgos definido, con el fin de alcanzar los objetivos del control identificados y que incluya la asignación de roles y responsabilidades.

Se apoya al ***ORGANISMO RECEPTOR DEL SERVICIO*** en la implantación de los controles anteriormente seleccionados que lleven a los objetivos de control.

Como parte de los trabajos de implantación del SGSI en el ***ORGANISMO RECEPTOR DEL SERVICIO*** y a partir del **SoA**, **Plan de Tratamiento de Riesgo** y **Programa de implementación** se realizan las siguientes actividades por parte de ***CONSULTOR REVISOR DEL SGSI***, tomando en cuenta los siguientes puntos para solventar los requerimientos de la etapa **DO** del modelo de mejora continua de Deming solicitado por el MAAGTIC:

Etapa de DO del Modelo de Deming

- Definición de los procedimientos y el sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles seleccionados y promover una mejora continua.

- En lo que se refiere a documentación Técnica se documentará los controles declarados en el SoA como aplicables al alcance del SGSI del ***ORGANISMO RECEPTOR DEL SERVICIO***, bajo los controles aplicables del **Anexo D de esta propuesta.**
- Verificación de la operación del SGSI
- Verificación de los recursos asignados al SGSI para el mantenimiento de la seguridad de la información.
- Apoyo en la implantación de los procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad de información.
- Se genera evidencia de madurez del SGSI

Los productos de esta fase, serán de acuerdo a los formatos siguientes:

OSGP – 2

- Anexo 8, Formato 6 "Documento de planeación para la implementación de mejora de procesos"

ASSI – 2

- Anexo 24, Formato 1 "Sistema de Gestión de Seguridad de la Información"
- Anexo 24, Formato 2 "Programa de implantación del Sistema de Gestión de Seguridad de la Información"
- Anexo 24, Formato 3 "Informe de la implantación del Sistema de Gestión de Seguridad de la Información"

AE – 1

- Anexo 4, Formato 1 "Objetivos e indicadores del sistema de evaluación de TIC", para los controles del SGSI.

3.4. Fase IV – Verificación

Como parte de lo trabajo de verificación del SGSI en el ***ORGANISMO RECEPTOR DEL SERVICIO*** se realizan las siguientes actividades por parte del ***CONSULTOR REVISOR DEL SGSI***, tomando en cuenta los siguientes puntos para solventar los requerimientos de la etapa del **CHECK** del modelo de mejora continua de Deming solicitado por MAAGTIC:

Etapa del CHECK – Monitoreo del SGSI:

- Se apoyara al ***ORGANISMO RECEPTOR DEL SERVICIO*** en la ejecución de procedimientos de revisión para:
  - Detección temprana de errores en los resultados generados por los procesos.
  - Identificación inmediata de brechas e incidentes de seguridad.
  - Determinar si las actividades desarrolladas por personal del ***ORGANISMO RECEPTOR DEL SERVICIO*** y la infraestructura tecnológica, para garantizar la seguridad de la información, operan en relación a lo previsto.
  - Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores.
  - Determinar si las acciones realizadas para resolver rechas de seguridad fueron efectivas.
  - El plan de recuperación de desastres.
- Se revisará la efectividad del SGSI, los resultados de las auditorias de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas; atendiendo al cumplimiento de la política y objetivos del SGSI.
- Se medirá la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

- Se revisarán las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior – requerimientos legales, obligaciones contractuales, y evidencia aplicable.
- Se realizará auditorías internas del SGSI.
- Se apoyará en la actualización de los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitoreo, revisión, y auditoria interna.
- Se registrará acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.
- Se desarrolla, implementa y documenta un proceso de auditoría interna, la cual se repetirá a intervalos planeados para determinar si los objetivos de control, controles y procedimientos del SGSI; cumplen los requerimientos del estándar MAAGTIC, legislaciones o regulaciones relevantes, requerimientos de seguridad de la información identificados en el análisis de riesgos y están efectivamente implantados y mantenidos.
- Se planea el programa de auditoria tomando en consideración el estatus, la importancia de los procesos y área a auditarse, así como los resultados de auditorías previas (en caso de existir).

Los productos de esta fase, de manera enunciativa más no limitativa, son los siguientes_

ASSI – 3

- Anexo 24, Formato 4 “Informe de Evaluación del Sistema de Gestión de Seguridad de la Información”
- Anexo 24, Formato 1 “Sistema de Gestión de Seguridad de la Información”

OSGP – 3

- Anexo 8, Formato 9 “Documento de planeación de evaluación”
- Anexo 8, Formato 12 “Solicitudes de mejoras de procesos”
- Repositorio de solicitudes de mejora

3.5. Fase V – Mantenimiento, Mejora

Como parte de las tareas a realizar en esta Fase se incluye la etapa del **ACT** del modelo de mejora continua de Deming.

Etapa del ACT

- Se apoyará en la implantación de las mejoras identificadas al SGSI.
- Se implantará un procedimiento de acciones correctivas que defina requerimientos para: identificar no conformidades de la implantación y/u operaciones del SGSI, determinar las causas de las no-conformidades; evaluar la necesidad de acciones para asegurar que las no-conformidades no vuelvan a ocurrir; registrar resultados de acciones llevadas a cabo; revisar las acciones correctivas realizadas.
- Se implantara un procedimiento de acciones preventivas que defina requerimientos para: identificar no-conformidades potenciales y sus causas; determinar e implementar acciones preventivas necesarias; registrar resultados de acciones tomadas: revisar las acciones correctivas realizadas; identificar cambio en los riesgos y asegurar que la atención de enfoque en riesgos nuevos o que hayan cambiado significativamente.

- Se apoyará en la realización de acciones preventivas y correctivas adecuadas, en relación a la norma MAAGTIC y a las lecciones aprendidas durante el proyecto.
- Se facilitara la comunicación de las acciones y mejoras a todas las parte interesadas con el nivel de detalle adecuado y acodará la forma de proceder.
- Apoyar en la verificación de las mejoras introducidas.
- Se lleva a cabo la revisión por la dirección.

Los productos de esta fase, de manera enunciativa más no limitativa, son los siguientes:

OSGP – 4

- Anexo 8, Formato 12 “Solicitudes de mejoras de procesos”

ASSI – 4

- Anexo 24, Formato 5 “Acción correctiva y preventiva”
- Anexo 24, Formato 6 “Informe de seguimiento de las acciones correctivas y preventivas”
- Anexo 24, Formato 1 “Sistema de Gestión de Seguridad de la Información”

4. PLAN DE TRABAJO

A continuación se presenta el plan de trabajo propuesto, para la implementación del SGSI del ***ORGANISMO RECEPTOR DEL SERVICIO*** con fundamento en el alcance descrito en esta propuesta.

5. PARTICIPANTES EN LOS TRABAJOS

- ***CONSULTOR REVISOR DEL SGSI*** incluye al personal declarado en esta propuesta.
- ***CONSULTOR REVISOR DEL SGSI*** trabajará en conjunto con el personal del ***ORGANISMO RECEPTOR DEL SERVICIO***.
- Se definen los perfiles y habilidades del RH interno y externo con el fin de evitar contratiempos y justificaciones.

Con las siguientes responsabilidades:

- **3 Consultores** – Responsables del desarrollo del SGSI del ***ORGANISMO RECEPTOR DEL SERVICIO***, con base en los requisitos del MAAGTIC.
- **3 Personal Interno** – Responsables de la supervisión y retroalimentación para llevar a cabo el presente proyecto**.**

PERFIL PARA PERSONAL EXTERNO

- Ingeniero en computación, sistemas o afín.
- Especializados en seguridad informática, deseable contar con certificaciones CISSP, SSCP, CISA, CISM, GIAC
- Con experiencia en seguridad de más de 2 años, con conocimientos de escaneo de puertos, análisis de riesgos, normativas de seguridad, auditorías de sistemas.

PERFIL PARA PERSONAL INTERNO

- Ingeniero en computación, sistemas o afín.
- Pertenecer a la Dirección de Tecnologías de la Información en el área de Seguridad informática.
- Especializados en seguridad informática, deseable contar con certificaciones CISSP, SSCP, CISA, CISM, GIAC

- Con experiencia en seguridad de más de 2 años, con conocimientos de escaneo de puertos, análisis de riesgos, normativas de seguridad, auditorías de sistemas.

6. ADMINISTRACIÓN DEL PROYECTO

6.1. MECANISMOS DE ADMINISTRACIÓN DE PROYECTOS

Como parte de la administración del proyecto realizará las siguientes tareas:

Inicio del proyecto.- ***CONSULTOR REVISOR DEL SGSI*** conducirá la junta inicial en donde se darán a conocer al grupo de trabajo, entregables en cada una de las tareas.

Despliegue del proyecto.- ***CONSULTOR REVISOR DEL SGSI*** es responsable del alcance descrito en esta propuesta, siendo parte esencial de dicho alcance, la identificación oportuna de riesgos que puedan comprometer tiempos y entregas

Transferencia de Conocimiento.- ***CONSULTOR REVISOR DEL SGSI*** será responsable de la transferencia de conocimiento lo largo del proyecto.

6.2. RESPONSABILIDADES DE AMBAS PARTES

Para cubrir el alcance descrito en este documento ***ORGANISMO RECEPTOR DEL SERVICIO*** & ***CONSULTOR REVISOR DEL SGSI*** tendrán las siguientes responsabilidades:

- ***ORGANISMO RECEPTOR DEL SERVICIO*** debe asignar un Líder de Proyecto que tenga acceso a personal clave de la organización.
- Personal clave del ***ORGANISMO RECEPTOR DEL SERVICIO*** debe de estar disponible para toma de decisiones críticas cuando estas se requieran.
- El grupo de trabajo del ***ORGANISMO RECEPTOR DEL SERVICIO*** debe permanecer como fue definido originalmente durante todo el proyecto.
- Si existen condiciones que puedan causar un retraso de información, ***CONSULTOR REVISOR DEL SGSI*** podrá convocar en un lapso de un día hábil al grupo de trabajo de ***CONSULTOR REVISOR DEL SGSI***.
- ***ORGANISMO RECEPTOR DEL SERVICIO*** se obliga a proporcionar en tiempo y forma los documentos y permisos requeridos por ***CONSULTOR REVISOR DEL SGSI*** para la realización de los trabajos.
- El personal clave del ***ORGANISMO RECEPTOR DEL SERVICIO*** será requerido en los tiempos que detallan en el plan de trabajo.

6.3. COMPROMISOS DEL CONSULTOR REVISOR DEL SGSI

- Firma de un acuerdo de confidencialidad con ***ORGANISMO RECEPTOR DEL SERVICIO*** según sea requerido, para el manejo de la información referente al alcance de los trabajos.
- Firma de contrato y cláusulas de confidencialidad y cumplimiento de controles de seguridad de información del ***ORGANISMO RECEPTOR DEL SERVICIO***.
- Cumplimiento con políticas y lineamientos del ***ORGANISMO RECEPTOR DEL SERVICIO*** en el manejo de la información durante y fuera de las instalaciones de la organización.
- Conducir o apoyar en juntas con el comité de dirección del ***ORGANISMO RECEPTOR DEL SERVICIO*** según sea requerido y acordado entre ambas partes.

- Dar seguimiento a los cambios que se requieran durante la ejecución de los trabajos.

6.4. REQUERIMIENTOS DEL CONSULTOR REVISOR DEL SGSI AL ORGANISMO RECEPTOR

- Lugares de trabajo para personal de ***CONSULTOR REVISOR DEL SGSI***.
- Acceso a las áreas de trabajo para los miembros del equipo a las instalaciones del ***ORGANISMO RECEPTOR DEL SERVICIO***.

6.5. CONTROL DE CAMBIOS

Los objetivos del "Control de Cambios" son:

- Evaluar el impacto de cambios en el alcance, planes de trabajo, recursos y precios.
- Proporcionar un vehículo formal para la aprobación de cualquier cambio hecho a este documento.
- Establecer el impacto de cualquier cambio.
- Proporcionar un registro de todos los cambios importantes que se hagan al alcance original.

En caso de que el ***ORGANISMO RECEPTOR DEL SERVICIO*** solicite un cambio en el alcance (a partir de lo acordado en el contrato y en esta propuesta), ambas partes revisarán el "Cambio".

Cuando el CONSULTOR REVISOR DEL SGSI detecte un cambio en el alcance, se generará un documento donde se especifique:

- Cambio
- Impacto en el plan de trabajo
- Recursos
- Costo (precio)

Lo entregará al ***ORGANISMO RECEPTOR DEL SERVICIO***, mismo que debe ser firmado por ambas partes a fin de dar aprobación por escrito al mismo.

Una vez que el ***ORGANISMO RECEPTOR DEL SERVICIO*** acepte el cambio se modificara su orden de pago conforme a lo acordado con el ***CONSULTOR REVISOR DEL SGSI***. En caso de que el ***ORGANISMO RECEPTOR DEL SERVICIO*** no acepte el cambio según lo estipulado en el documento, las partes cumplirán sus obligaciones según lo estipulado en el contrato.

7. DÍAS DE MANTENIMIENTO

En la siguiente tabla se describe el número de días por mantenimiento semestral y los 6 servicios solicitados durante un periodo de 3 años, que se han incluido como parte del mantenimiento al SGSI del ***ORGANISMO RECEPTOR DEL SERVICIO***.

	AÑO 1		AÑO 2		AÑO 3	
Etapas	Mtto 1	Mtto 2	Mtto 3	Mtto 4	Mtto 5	Mtto 6
Días de Etapa de PLAN	10	10	10	10	10	10
Días de Etapa de DO	20	20	20	20	20	20
Días de Etapa de CHECK	5	5	5	5	5	5
Días de Etapa de ACT	5	5	5	5	5	5
Días consultor	40	40	40	40	40	40

La implantación del SGSI con base en requisitos del MAAGTIC se consume 133 días de los días mantenimiento del *ORGANISMO RECEPTOR DEL SERVICIO*.

ANEXO A. 5.4.1 Operación del sistema de gestión y mejora de los procesos de la UTIC

5.4.1.1 Objetivos del proceso

General:

Establecer y operar un sistema de gestión y mejora de los procesos de la UTIC en el que se verifiquen, monitoreen y evalúen los procesos y se consideren las acciones de mejora necesarias para una operación eficiente de la UTIC.

Específicos:

1. Contar con un mecanismo que dé seguimiento a los procesos del "Marco rector de los procesos en materia de TIC", con el propósito de tener un mejor control de los mismos.

2. Establecer y ejecutar mejoras para la ejecución de los procesos, apoyándose de los resultados de la operación de indicadores que se generan en los diversos procesos y la ejecución de evolución sobre los mismos, a fin de optimizar la operación del "Marco rector de los procesos en materia de TIC".

5.4.1.2 Descripción del proceso

5.4.1.2.1 Descripción de las actividades del proceso

OSGP-1: Implementar el Sistema de Gestión y Mejora de los Procesos de la UTIC

DESCRIPCIÓN:

Desarrollar el sistema de gestión y mejora de los procesos de la UTIC con un enfoque sistémico alineado al "Marco rector de procesos en materia de TIC".

FACTORES CRITICOS:

El responsable del proceso de la operación del sistema de gestión y mejora de los procesos de la UTIC deberá:

1. Establecer y mantener el repositorio de activos de procesos, así como los criterios para incorporar elementos al mismo.

2. Integrar en el repositorio de activos de procesos, características esenciales de los procesos del "Marco rector de procesos, considerando por lo menos la información siguiente:

   - Objetivo y propósito de cada uno de los procesos.
   - Responsables de cada uno de los procesos.
   - Límites: Inicio y fin de cada uno de los procesos.
   - Entradas y salidas.
   - Proveedores y usuarios de cada uno de los procesos.
   - Mecanismos de medición: indicadores de cada uno de los procesos.
   - Recursos de los procesos: Humanos, financieros, infraestructura y ambiente de trabajo.
   - Representaciones gráficas: Mapa general del proceso.

- Factores críticos de cada uno de los procesos.
- Interrelaciones con otros procesos: Especificar secuencias e interacciones de los procesos con el propósito de asegurar que existe una apropiada integración entre ellos, incluyendo conexiones con procesos internos y externos.

Este factor crítico se debe apegar al proceso de Administración del conocimiento.

3. Modelar en forma gráfica, a través de un Mapa General de Procesos, el Sistema de Gestión y Mejora de los procesos de la UTIC, mostrando la jerarquía, relación e interacción entre los mismos.

4. Definir y comunicar oportunamente metas y objetivos específicos, medibles, viables y orientados a resultados para cada proceso y que se sustenten en métricas adecuadas.

5. Asignar a un responsable para cada proceso.

6. Completar las especificaciones de los procesos, estableciendo para cada uno, frecuencia y resultados esperados. Proveer una secuencia lógica pero flexible y escalable de actividades, que lleve a los resultados deseados y que sea lo suficientemente ágil para manejar las excepciones y emergencias.

7. Verificar los roles, actividades y responsabilidades en la ejecución de los procesos, incluyendo la documentación que se genere en los mismos.

8. Informar, a los involucrados del proceso, los resultados que se hayan obtenido de la verificación en cada uno de los procesos.

9. Definir los documentos y los activos del proceso que se encontraran bajo control de cambios y de versiones.

10. Definir los objetivos de los procesos, las actividades de verificación, validación, monitoreo, inspección, pruebas específicas y criterios de aceptación para los productos de cada proceso.

11. Elaborar registros para proveer evidencia sobre el cumplimiento de requerimientos de los procesos y sus productos.

12. Identificar un conjunto de métricas que permitan apreciar los resultados y el desempeño del proceso e implementar acciones para corregir desviaciones respecto a las metas, cuando sea necesario.

13. Alinear métricas, objetivos y métodos con el enfoque de monitoreo global del rendimiento de TIC, establecido en el proceso de Administración de la evaluación de TIC.

14. Establecer y actualizar los modelos de ciclo de vida aplicables.

15. Establecer y actualizar las guías de adaptación de manera que permitan crear un “proceso específico” valido únicamente para que responda a las necesidades específicas de los diversos tipos de proyecto.

16. Establecer los estándares de ambiente de trabajo para la operación de los procesos y proyectos de la UTIC considerando: instalaciones, espacio de trabajo, herramientas, relación de productos asociadas, software e infraestructura.

17. Integrar en el documento de administración del proceso (también llamado PLAN DE CALIDAD DEL PROCESO, según ISO 9001) los elementos necesarios para la dirección, realización y control del proceso.

18. Revisar de manera periódica las necesidades de definición y control de los procesos de TIC de la institución.

- Anexo 8 Formato 1 “Mapa General del Proceso”
- Anexo 8 Formato 2 “Documento de Administración del Proceso”
- Anexo 8 Formato 3 “Modelos de Ciclo de Vida”
- Anexo 8 Formato 4 “Guías de Adaptación”
- Anexo 8 Formato 5 “Estándares de Ambiente de Trabajo”
- Repositorio de activos de procesos.

OSGP-2: Ejecutar la planeación de implementación de mejora de los procesos y operar el Sistema de Gestión y Mejora de los Procesos de la UTIC.

DESCRIPCIÓN:

Elaborar los documentos para la implementación de los procesos y operar el Sistema de Gestión y Mejora de los procesos de la UTIC.

FACTORES CRITICOS:

El responsable del proceso de Operación del Sistema de Gestión y Mejora de los Procesos de la UTIC deberá:

1. Elaborar las estrategias y medidas de acción detallados en un documento de planeación para la implementación de mejora de procesos, considerando al menos los siguientes elementos:

   - Mapa General del Proceso.
   - Documento de Administración del Proceso.
   - La información contenida en el repositorio de activos de procesos.
   - Las solicitudes de mejora, en caso de haberse recibido.
   - Los indicadores de rendimiento.
   - Los recursos de TIC.
   - Los proyectos de servicios de TIC en desarrollo y compromisos de la UTIC.
   - Las áreas de la UTIC a las cuales se les aplica una acción de mejora en el proceso.

2. Elaborar el proyecto de implementación de mejora de procesos y de despliegue, siguiendo el proceso de Administración de proyectos de TIC, el cual contendrá:

   - La ejecución de pruebas piloto de las mejoras de proceso seleccionadas.
   - La revisión y negociación las acciones y compromisos con los involucrados relevantes y con los equipos involucrados.
   - El establecimiento de equipos de trabajo para el proyecto.

- La verificación de que los proyectos, servicios y actividades no sean afectados en su ciclo de vida incluyendo:
  - Servicios en etapa de diseño en su ejecución.
  - Proyectos que inician.
  - Proyectos activos que se podrían beneficiar de la implementación.
  - Actividades de operación críticas en la provisión de los servicios de TIC.

3. Comunicar el proyecto de implementación de mejora de procesos a los involucrados.

4. Ejecutar el proyecto de implementación de mejora de procesos y operar el Sistema de Gestión y Mejora de los Procesos de la UTIC, procurando la realización de las siguientes actividades:

   - Asesoría y soporte en la adaptación de los procesos de acuerdo a las necesidades propias de los proyectos y servicios.
     - Registrar las adaptaciones a los procesos , incluyendo evidencias
     - Comunicar las adaptaciones efectuadas
   - Asesoría sobre el uso de los activos de los procesos.

5. Dirigir, supervisar y controlar el trabajo de los equipos de trabajo y de los involucrados para monitorear el avance y los resultados del proyecto de implementación de mejora de procesos.

6. Recopilar las lecciones aprendidas en la definición, pilotaje, implementación y despliegue de las mejoras de los procesos y ponerlas a disposición de los involucrados e interesados.

RELACIÓN DE PRODUCTOS

- Anexo 8 Formato 6 “Documento de Planeación para la Implementación de Mejora de Procesos”
- Anexo 8 Formato 7 “Proyecto de Implementación de Mejora de Procesos”
- Anexo 8 Formato 8 “Lecciones Aprendidas”
- Repositorio de activos de procesos
- Repositorio de métricas de procesos

OSGP-3: Monitorear y evaluar la operación del Sistema de Gestión y Mejora de los Procesos de la UTIC.

DESCRIPCIÓN:

Dar seguimiento y evaluar la operación del Sistema de Gestión y Mejora de los Procesos de la UTIC.

FACTORES CRITICOS

Se deberá establecer un grupo de trabajo de aseguramiento de calidad en las Instituciones, integrado por diversos servidores públicos de la UTIC.
Dicho grupo deberá:

1. Contar con el compromiso de los involucrados para la evaluación de los procesos de la UTIC con el propósito de :

- Obtener un diagnostico actual de los procesos de la UTIC.
- Obtener un inventario de las capacidades del personal que interviene en la ejecución de los procesos.
- Identificar los procesos que tienen oportunidades de mejora.
- Confirmar en avance del proyecto de implementación de mejora de procesos y hacer visibles los beneficios de mejora de procesos.
- Generar conciencia del valor y de los beneficios potenciales de la inversión en el establecimiento y mejora de los procesos.
- Motivar a los involucrados y facilitar la aceptación del cambio.

2. Monitorear y medir los productos/servicios de los procesos:

   - Verificar que los requerimientos se han cumplido.

3. Conservar evidencia de la conformidad con los criterios de aceptación. Monitorear y medir los procesos:

   - Aplicar métodos apropiados para dar seguimiento a los procesos. Los métodos que se utilicen deberán evidenciar la eficiencia de los procesos.
   - Implementar acciones para corregir la desviación y eliminar, de ser posible, la causa raíz, cuando no se obtengan los resultados esperados.
   - Conservar evidencia de la conformidad con los criterios de aceptación.
   - Alinear las capacidades de los involucrados con los procesos que operan, en apego a los procesos de establecimiento del modelo de gobernabilidad de TIC y de integración y desarrollo de personal.

4. Elaborar el documento de planeación de evaluación, así como conducir, al menos una vez al año, las evaluaciones en intervalos planeados, para determinar si los procesos establecidos se apegan al “Marco rector de procesos en materia de TIC”, con base en los niveles de evaluación previstos para cada proceso:

   - Definir los criterios, el alcance, la frecuencia y los métodos de las evaluaciones.
   - Promover la objetividad de las evaluaciones.
   - Seleccionar a los evaluadores de calidad de manera que se asegure la objetividad y la imparcialidad de la evaluación. Los evaluadores no deberán evaluar su propio trabajo.

5. En caso que la evaluación tenga como propósito demostrar el cumplimiento de un estándar ante terceros (tal como CMMI, ISO 9001, ISO 20000, ISO 27001, etc.) el evaluador deberá estar acreditado ante las organizaciones que determinen los propietarios de los derechos de autor del estándar que se trate.

   - Establecer el programa de evaluaciones tomando en cuenta tanto el estado y la importancia de los procesos y las áreas de la UTIC a ser evaluadas como los resultados de evaluaciones anteriores.
   - Considerar la evaluación periódica de los procesos.
   - Elaborar análisis comparativos entre los procesos evaluados.
   - Registrar y comunicar los resultados de las evaluaciones.
   - El responsable del proceso de evaluado procurará que se efectúen acciones relacionadas con los hallazgos encontrados durante las evaluaciones.

6. Integrar en el reporte de evaluación de procesos lo siguiente:

   - Los resultados de la evaluación.

- Los hallazgos (el estado de las “no conformidades” provee un indicador de la calidad de los procesos de la UTIC).
- Las oportunidades de mejora identificadas, por proceso y de diversas fuentes, como lo son:

    - Las lecciones aprendidas en la implementación de los procesos.
    - Propuestas y solicitudes de mejoras de procesos elaboradas por los involucrados en la administración, control y ejecución del proceso.
    - Resultados de las evaluaciones efectuadas a los procesos.
    - Informes de la información de medición y análisis de la evaluación de los procesos.
    - Resultados de análisis comparativo con otros procesos del “Marco Rector de los Procesos en Materia de TIC” del presente manual.
    - Recomendaciones de otras instancias de la Administración Pública Federal.

7. Registrar y comunicar los resultados obtenidos para la definición de las acciones de mejora a ser implementadas.

RELACIÓN DE PRODUCTOS:

- Anexo 8, Formato 9 “Documento de planeación de evaluación
- Anexo 8, Formato 10 “ Análisis Comparativo”
- Anexo 8, Formato 11 “Reporte de Evaluación de Procesos”
- Anexo 8, Formato 12 “Solicitudes de Mejoras de Procesos”
- Repositorio de solicitudes de mejora

OSGP-4: Ejecutar las acciones de mejora a los productos de la UTIC.

Descripción:

Se ejecutan las acciones de la mejora a los productos del “Marco Rector de Procesos en Materia de TIC”.

Factores Críticos:

1. Se establecerá un grupo de trabajo de procesos y mejora continua de la UTIC en las instituciones, integrado por diversos servidores públicos de la UTIC.

Dicho grupo será el responsable de administrar las mejoras a los procesos de la UTIC, de manera ordenada y orientado al beneficio de la institución, mediante un proceso de control de cambios.

2. El grupo de trabajo de procesos y mejora continua de la UTIC deberá:

    - Registrar en el repositorio de solicitudes de mejora las Solicitudes de Mejora de Procesos.

Analizar, priorizar y seleccionar las propuestas de mejora, considerando los criterios siguientes:

- Menor costo y horas de trabajo.
- Mayores beneficios tangibles e intangibles resultantes de las propuestas de mejora.
- Mayor contribución de las mejoras propuestas al cumplimiento del PETIC.
- Mínimas barreras potenciales a la implementación de las propuestas.

Documentar las mejores propuestas como iniciativas de TIC o proyectos de mejora, conforme a lo establecido en el proceso de Administración del Portafolio de proyectos de TIC, para su evaluación, selección y autorización correspondiente.

Dar seguimiento a las “no conformidades” hasta su cierre y validar que las acciones correctivas implementadas son efectivas.

Elaborar el documento que contenga el resultado de mejoras implementadas.
Iniciar un nuevo ciclo del proyecto, si las acciones realizadas no tiene el resultado esperado, para lo cual se deberá regresar a la actividad del OSGP-1, para determinar las necesidades del sistema de gestión y mejora de los procesos de la UTIC.
Integrar la información del resultado de mejoras implementadas.

RELACIÓN DE PRODUCTOS

-
- Anexo 8, Formato 12 “Solicitudes de Mejoras de Procesos”¨
- Anexo 8, Formato 13 “Informes de Medición y análisis”
- Anexo 8, Formato 14 “Resultado de Mejoras Implementadas”
- Repositorio de solicitudes de mejora.

TIEMPO TOTAL DEL PROCESO: VARIABLE.

5.4.1.2.2 Mapa General del Proceso

Diagrama de flujo de información

Se encuentra disponible en la dirección siguiente: www.maaagtic.gob.mx

Diagrama de Flujo de actividades

Se encuentra disponible en la dirección siguiente: www.maagtic.gob.mx

5.4.1.2.3 Descripción de roles

Responsable de mejora de procesos

- Coordina y administra las tareas de evaluación, definición, implementación y despliegue de las iniciativas/proyectos de mejora de los procesos de la UTIC, así como la administración de las solicitudes de mejora y lecciones aprendidas.

Grupo de aseguramiento de calidad

- Coordina las actividades de evaluación, desarrolla la implementación de actividades y se asegura de su ejecución.
- Reporta al Responsable de mejora de los procesos los resultados de las actividades de evaluación.

Evaluador de calidad

- Responsable de realizar actividades del documento de planeación de evaluación.

Grupo de trabajo de mejora continua de TIC

- Responsable de planear y desplegar el documento de planeación de implementación de mejora.
- Apoya en la definición de los procesos de la UTIC y asesora en su operación.

Responsable del proceso

- Responsable de asegurar que el proceso se ejecute de acuerdo al documento de administración del proceso y de que este cumple con sus objetivos.

5.4.1.3 INDICADORES
5.4.1.4

	INDICADOR 1	INDICADOR 2
NOMBRE	Cumplimiento de procesos apegados al marco rector.	Resultados del sistema de gestión y mejora de los procesos de la UTIC.
OBJETIVO	Conocer la eficiencia del proceso mediante el cumplimiento del “Marco Rector de Procesos en Materia de TIC”.	Conocer la eficiencia del proceso mediante las acciones de mejora implementadas.
DESCRIPCIÓN	Medir el porcentaje de cumplimiento de procesos conforme al “Marco Rector de Procesos en Materia de TIC”.	Medir los resultados del sistema en cuanto a implementación de mejoras.
DIMENCIÓN	Eficiencia	Eficiencia
TIPO	De gestión	De gestión
FORMULA	% de eficiencia= (número de procesos que se efectúan con apego al”Marco rector”/número de procesos adoptados del “Marco rector de procesos en materia de TIC”)*100.	% de eficiencia= (Total de mejoras implementadas/Total de mejoras identificadas)*100

RESPONSABLE	Responsable del sistema de gestión y mejora de los procesos de la UTIC.	Responsable de mejora de procesos.
FRECUENCIA DE CÁLCULO	Semestral	Semestral

5.4.1.4 REGLAS DEL PROCESO

1. La UTIC regirá su gestión con estricto apego a los procesos del “Marco Rector de Procesos en Materia de TIC”, contenidos en el presente Manual.

2. Los procedimientos e instrucciones de trabajo que establezca la UTIC deberá estar alineados a los procesos del “Marco Rector de Procesos en Materia de TIC”.

3. Serán extensivas a este proceso las disposiciones de seguridad de la información establecidas por medio del SGSI.

4. La evaluación de este proceso, deberá realizarse de acuerdo a lo establecido en el proceso de Administración de la evaluación de TIC.

5. Los roles y responsabilidades de este proceso deberán definirse mediante el proceso de establecimiento del modelo de gobernabilidad de TIC.

6. El responsable de la UTIC, mediante este proceso, deberá verificar que los participantes en la ejecución de los proceso del “Marco Rector de Procesos en Materia de TIC” del presente manual cuenten con las capacidades, habilidades y conocimientos para realizar las actividades al rol que les sea asignado.

7. El responsable de la UTIC para cada proceso deberá revisar y aprobar el documento de Administración del proceso correspondiente.

8. El titular de la UTIC, mediante este proceso deberá asignar un responsable de administrar cada uno de los procesos el “Marco Rector de Procesos en Materia de TIC” del presente manual.

9. El administrador de este proceso realizará evaluaciones semestrales documentadas a fin de verificar que la operación de los procesos corresponda al documento de administración del proceso.

5.4.1.5 DOCUEMTACIÓN SOPORTE DEL PROCESO

Los anexos señalados en este proceso serán publicados en la dirección siguiente: www.maagtic.gob.mx

ANEXO B. 5.9.4 ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

5.9.4.1 OBJETIVOS DEL PROCESO

General

Establecer los mecanismos que permitan la administración de la seguridad de la información de la institución contenida en medios electrónicos y sistemas informáticos.

Específicos

Establecer un Sistema de Gestión de Seguridad de la Información (SGSI) que protege la información de la institución contenida en medios electrónicos y sistema informáticos, contra acceso y usos no autorizados, con la finalidad de conservar su confidencialidad, integridad y disponibilidad.

5.9.4.2 DESCRIPCIÓN DEL PROCESO

5.9.4.2.1 Descripción de las actividades del proceso

ASSI-1 Diseño del Sistema de Gestión de Seguridad de la Información (SGSI)

Descripción

Definir los objetivos y directrices para establecer un Sistema de Gestión de la Seguridad de la Información contenida en medios electrónicos y sistemas de informáticos de la institución en términos de las disposiciones jurídicas aplicables.

Factores críticos:

El responsable del SGSI deberá:

1. Definir el alcance del SGSI, que establezca límites de protección desde la perspectiva institucional, para proteger adecuadamente los activos tecnológicos y sistemas informáticos, incluyendo medios electrónicos de almacenamiento y de comunicación y la información contenida en los mismos.

2. Involucrar a la unidad de responsabilidades de la información contenida en medios electrónicos y sistemas informáticos, ya que son fuente principal para establecer el alance, riesgos, vulnerabilidades, amenazas e impacto de la seguridad en la información de la institución.

3. Definir los roles y responsabilidades del personal que participa en el diseño del SGSI.

4. Realizar un diagnóstico de los requerimientos de seguridad de la información de la institución, a través de un análisis de riesgos de seguridad informática que valore sus activos, conociendo las vulnerabilidades y amenazas que pueda sufrir la información contenida en medios electrónicos y sistemas de información.

5. Asociar cada riesgo con las estrategias y/o objetivos de la institución, estrategias de seguridad informática, considerando los principios de integridad, confidencialidad y disponibilidad de la información.

6. Elaborar el programa de mitigación de riesgos que contenga las estrategias de corto, mediano y largo plazo para enfrentar y mitigar los riesgos de seguridad de la información identificados en medios electrónicos y sistemas informáticos.

7. Definir métricas y controles de verificación de cumplimiento de los requerimientos de seguridad de la información identificados en medios electrónicos y sistemas informáticos.

8. Elaborar el programa de implantación del SGSI que incluya los procesos y procedimientos que permitan su adecuada operación.

Relación de productos

- Anexo 24, Formato 1 “Sistema de Gestión de Seguridad de la Información”.
- Anexo 24, Formato 2 “Programa de implantación del Sistema de Gestión de la Seguridad de la Información”.

ASSI-2 Implementar el Sistema de Gestión de la Seguridad de la Información.

Descripción

Asegurar que los controles, procesos y procedimientos del SGSI sean implementados de manera que se cumpla con los requerimientos de seguridad establecidos en las disposiciones jurídicas aplicables y para mitigar los riesgos identificados.

Factores críticos:

El responsable del SGSI deberá:

1. Ejecutar, dar seguimiento y actualizar el estatus del Programa de Implantación del SGSI en la institución.

2. Implementar y operar los controles de seguridad documentados en el SGSI.

3. Documentar y comunicar las acciones realizadas en el SGSI.

Relación de Productos

- Anexo 24, Formato 1 “Sistema de Gestión de la Seguridad de la Información”.
- Anexo 24, Formato 2 “Programa de Implantación del Sistema de Gestión de la Seguridad de la Información”.
- Anexo 24, Formato 3 “Información de la implantación del Sistema de Gestión de la Seguridad de la Información”.

ASSI-3 Evaluar el Sistema de Gestión de la Seguridad de la Información.

Descripción:

Evaluar y medir el rendimiento de los procesos del SGSI

Factores críticos:

Se deberá establecer en la institución un grupo de trabajo para la seguridad de la información, integrado para servidores públicos de la UTIC y por los usuarios del SGSI. El grupo de trabajo para la seguridad de la información, deberá:

1. Realizar revisiones para revisar la eficiencia y la eficacia de los controles implementados en el SGSI.

2. Medir la efectividad de los controles de seguridad para verificar que se hayan cumplido los requerimientos de seguridad de información.

3. Efectuar el monitoreo de la seguridad de la información en medios electrónicos y sistemas informáticos para validar la efectividad del SGSI.

4. Revisar los intentos exitosos y no exitosos de violaciones e incidentes de seguridad.

5. Documentar y comunicar las acciones de evaluación del SGSI a los usuarios del SGSI.

Relación de productos

- Anexo 24, Formato 4 “Informe de Evaluación del Sistema de Gestión de la Seguridad de la Información”.
- Anexo 24, Formato 1 “Sistema de Gestión de Seguridad de la Información”.

ASSI-4 Mejorar el Sistema de Gestión de la Seguridad de la Información

Descripción:

Mejorar la seguridad de la información, a través de la aplicación de las acciones preventivas y correctivas basadas en los resultados de revisiones, con el propósito de lograr la mejora continua del Sistema de Gestión de la Seguridad de la Información.

Factores Críticos

Grupo de trabajo de seguridad de la información deberá:

1. Establecer las acciones preventivas y correctivas con la finalidad de minimizar los riesgos de seguridad de la información identificados.
2. Implantar y dar seguimiento a las acciones correctivas y preventivas.
3. Documentar las acciones realizadas en el SGSI.

Relación de productos

- Anexo 24, Formato 5 “Acción Correctiva y Preventiva”.
- Anexo 24, Formato 6 “Informe de Seguimiento de las Acciones Correctivas y Preventivas”.
- Anexo 24, Formato 1 “Sistema de Gestión de Seguridad de la Información”.

Tiempo total del proceso: VARIABLE

5.9.4.2.2 Mapa general del proceso

Diagrama de flujo de información

Se encuentra disponible en la siguiente dirección www.maagtic.gob.mx

Diagrama de flujo de actividades

Se encuentra disponible en la siguiente dirección www.maagtic.gob.mx

5.9.4.2.3 Descripción de roles

Grupo de trabajo de seguridad de la información:

- Evalúa la seguridad de la información de la institución contenida en medios electrónicos y sistemas informáticos.
- Mejora la seguridad de la información de la institución contenida en medios electrónicos y sistemas informáticos.

Responsable de la seguridad de la información

- Establece el sistema de gestión de la información de la institución.
- Implanta y opera el Sistema de Gestión de Seguridad de la Información de la institución.

Usuarios del Sistema de Gestión de la Seguridad de la Información

- Servidores públicos que hacen uso de los activos de información contenida en medios electrónicos y sistemas de información.

5.9.4.3 INDICADORES

	INDICADOR
NOMBRE	Resultados del proceso de seguridad de la información.
OBJETIVO	Medir los resultados de la operación del Sistema de Gestión de Seguridad de la Información.

DESCRIPCIÓN	Medir la eficiencia del proceso mediante el conteo del número de incidentes de seguridad corregidos vía el Sistema de Gestión de Seguridad de la Información.
DIMENCIÓN	Eficiencia
TIPO	De gestión
FORMULA	% de eficiencia= (número de incidentes de seguridad corregidos mediante las acciones correctivas y preventivas del proceso y el sistema)/(Número de incidentes de seguridad registrados)*100
RESPONSABLE	Responsable de la seguridad de la información.
FRECUENCIA DE CÁLCULO	Semestral

5.9.4.4 Reglas del proceso

La UTIC verificara que el grupo de trabajo para la dirección de la TIC apoye las iniciativas y estrategias de seguridad de la información contenida en medios electrónicos y sistemas informáticos.

1. La UTIC deberá iniciar y controlar la implementación de la seguridad de la información contenida en medios electrónicos y sistemas informáticos dentro de la institución a través de la implantación de un SGSI.

2. La UTIC será la responsable de la seguridad de los recursos y activos de TIC, por lo que procurará que la infraestructura y servicios que se utilicen, administren o desarrollen cumplan con lo previsto en este proceso.

3. La evaluación de este proceso deberá realizarse de acuerdo a lo establecido en el proceso de Administración de la evaluación de TIC.

4. Los roles y responsabilidades de este proceso deberán definirse mediante el proceso de establecimiento del modelo de gobernabilidad de TIC.

5. Las reglas mínimas que deberán ser observadas por la UTIC, relacionadas con la seguridad de la información contenida en medios electrónicos, se encuentran disponibles en www.maagtic.gob.mx

5.9.4.5 Documentación de soporte del proceso

Los anexos señalados en este proceso serán publicados en la dirección siguiente www.maagtic.gob.mx

5.2.2 Administración Riesgos TIC

5.2.2.1 Objetivos del Proceso

General:

Disminuir el impacto de los riesgos adversos que potencialmente podrían afectar el logro de los objetivos de la institución en materia de TIC.

Específicos:

1. Establecer en la UTIC un sistema que permita identificar, analizar, evaluar, atender y monitorear los riesgos en materia de TIC.

2. Establecer mediante el sistema previsto en el numeral anterior, los medios que permitan tomar decisiones de manera informada y oportuna sobre la mitigación de los riesgos en materia de TIC.

5.2.2.2 Descripción del Proceso

5.2.2.2.1 Descripción de las actividades del proceso

ARTI-1 Establecer las directrices del proceso y el Sistema de Administración de Riesgo de TIC.

Descripción:

Establecer las directrices del proceso de Administración de Riesgos de TIC y el Sistema de Administración de Riesgos de TIC.

Factores Críticos:

Se integrará un grupo de trabajo de riesgos de TIC en cada una de las instituciones, conformado por servidores públicos de la UTIC.

La UTIC al establecer el grupo de trabajo de riesgos de TIC deberá:

- Acordar y definir el rol y responsabilidades del grupo de trabajo de riesgos de TIC.
- Establecer y comunicar el alcance, objetivos, roles y responsabilidades de los integrantes del grupo de trabajo de riesgos de TIC.

1. El grupo de trabajo de riesgos de TIC deberá: identificar en el ambiente interno y externo los riesgos, que en materia de TIC, podrían influir en la institución:

   - En el ambiente externo los aspectos que podrían considerar son, entre otros:
     - Legales, financieros, tecnológicos, económicos, naturales y competitivos, tanto a nivel federal y estatal, como en el ámbito internacional.
       - Tendencias e impulsores externos que tienen impacto en los objetivos de la institución en materia de TIC.
       - Percepciones y valores que los involucrados externos tienes de la institución en materia TIC.

   - En el ambiente interno los aspectos que podrán considerar entre otros son:
     - Los estándares y modelos de referencia adoptados por la institución en materia de TIC.
     - Las políticas, objetivos y estrategias definidas en materia de TIC.
     - Las soluciones tecnológicas y flujos existentes de información en la institución, así como en aquellos procesos del "Marco Rector de Procesos en Materia de TIC" en donde se tomen decisiones.

2. Documentar y difundir una directriz rectora en donde se definan los antecedentes, sustentos y justificaciones de la necesidad de implantar, a través de la UTIC, la administración de los riesgos de TIC en la institución.
   La directriz rectora deberá:

   - Mantenerse alineada con la estrategia de la administración de riesgo de la institución.
   - Establecer los roles y responsabilidades de los servidores públicos que intervienen en el presente proceso.
     - Integrar los requerimientos regulatorios aplicables.
     - Contener, entre otros, elementos siguientes:
       - Umbrales de tolerancia al riesgo en materia de TIC de la institución.
       - Mecanismos o métodos que medirán el presente proceso y la administración de riesgos en materia de TIC.
       - Procesos, métodos y herramientas que se usaran para administrar los riesgos en materia de TIC.
       - Acciones que serán tomadas para corregir las desviaciones de los límites de exposición al riesgo, así como los ajustes preventivos a los niveles de tolerancia al riesgo.
     - Establecer la forma y periodicidad en que se informara a los grupos de trabajo involucrados y a los usuarios, sobre los riesgos en materia de TIC a los que se encuentran expuestos los procesos y servicios que utilizan.
     - Contener las acciones que deberán aplicarse cuando pudiera existir incumplimiento en la administración de un riesgo en materia de TIC.
     - Establecer criterios para incluir consideraciones de riesgos en materia de TIC, en la toma de decisiones estratégicas de la institución.
     - Definir la periodicidad con la que se efectuara la revisión de la Directriz Rectora y, en su caso, respecto a su actualización.
     - Definir los reportes de gestión del proceso de administración de riesgos de TIC y la periodicidad con la que se elaborarán y comunicarán.
     - Establecer la forma en que se difundirá la directriz rectora.

3. Enviar para revisión y, en su caso, aprobación de la directriz rectora del proceso de administración de riesgos de TIC al grupo de trabajo para la dirección de TIC.

   El Sistema de administración de riesgos de tic se constituye mediante la instrumentación y operación de la directriz rectora.

Relación de productos:

- Anexo 5, Formato 1 “Descripción de roles y responsabilidades del grupo de trabajo de riesgos de TIC”
- Anexo 5, Formato 2 “Directriz rectora del proceso de administración de riesgos de TIC”

ARTI-2 Evaluar los riesgos de TIC

Descripción:

Evaluar los riesgos de TIC que permitan identificar los impactos sobre los procesos y los servicios de la institución.

Factores Críticos:

El grupo de trabajo de riesgos de TIC deberá:

1. Recopilar los datos relevantes relacionados con los riesgos de TIC, tales como:
   a) Incidentes que hayan tenido algún impacto en la institución.
   b) Riesgos del activo o recurso a evaluar.
   c) Controles actualmente implementados en los activos o recursos a evaluar.

2. Identificar y clasificar las amenazas y riesgos en materia de TIC, conforme a lo que sigue:

   - No causadas por el hombre:
     - Fallas de TIC o de infraestructura de soporte.
     - Desastres naturales.
   - Causados por el hombre
     - Dolosas, son aquellas con la intención de causar un daño.
     - Culposas, son aquellas que sin intención alguna se causa un daño.

3. Identificar los factores de riego que afecten a la institución los cuales pueden clasificarse en :

   - Financieros.
   - Niveles de servicios en materia de TIC.
   - Imagen o reputación en materia de TIC.
   - Regulatorios.

4. Identificar y analizar escenarios de riesgo de tic que permitan evaluar y obtener los impactos potenciales considerando, entre otros, los elementos siguientes:

   - Servicios.
   - Procesos.
   - Datos (operativos, nómina, contables, entre otros).
   - Software (sistemas, aplicaciones, entre otros).

- Hardware.
- Equipos informáticos que hospedan datos aplicaciones y servicios.
- Equipos de comunicaciones.
- Dispositivos de almacenamiento.
- Usuarios y de personal externo a la institución.

Para cada escenario de riesgo se debe definir y acordar la prioridad para su implantación, algunos de los parámetros que pueden ser considerados para dicha prioridad son:

- Severidad del riesgo.
- Nivel de impacto de la implantación
- Costo de la implantación

5. Integrar las matrices de riesgo de TIC, que son necesarias, con la información referida en los numerales de 1 a 4 anteriores.

Relación de productos

- Anexo 5, Formato 3 “Matrices de Riesgo de TIC”
- Repositorio de riesgos TIC.

ARTI-3 Responder a los riegos TIC

Descripción:

Responder a los riesgos de TIC de acuerdo a las decisiones para su tratamiento y los criterios de priorización.

Factores Críticos:

El grupo de trabajo de riesgo de TIC deberá:

1. Identificar el nivel de severidad del riesgo.

2. Identificar opciones para el tratamiento y control del riesgo a efecto de tomar decisiones para :
   a) Aceptar el riesgo: No se efectúa ninguna acción debido a que el nivel de riesgo está dentro de los niveles aceptables por la entidad o dependencia.
   b) Evitar el riesgo: Se elimina la causa que produce el riesgo.
   c) Transferir el riesgo: Se transfiere y comparte el riesgo.
   d) Mitigar el riesgo: Se implementan acciones para reducir el riesgo a un nivel aceptable.

3. Identificar acciones preventivas y correctivas y correlacionarlas para cada uno de los escenarios de riesgos identificados. Estas acciones se deberán integrar a las declaraciones de aplicabilidad.

4. Definir programas de mitigación del riesgo, lo cuales consideran las acciones para implantar los controles de riesgos en las declaraciones de aplicabilidad.

5. Definir un programa de contingencia para hacer frente a los eventos o incidentes de los riesgos identificados que en materia TIC pudieran presentarse.

Relación de productos:

- Anexo 5, Formato 4 “Declaraciones de Aplicabilidad”
- Anexo 5, Formato 5 “Programas de Mitigación de Riesgos”
- Anexo 5, Formato 6 “Programas de Contingencias”
- Repositorios de Riesgos de TIC.

TIEMPO TOTAL DEL PROCESO: *VARIABLE*

5.2.2.2.2 Mapa General del Proceso

Diagrama de flujo de información
Se encuentra disponible en la siguiente dirección www.maagtic.gob.mx
Diagrama de flujo de actividades
Se encuentra disponible en la siguiente dirección www.maagtic.gob.mx

5.2.2.2.3 Descripción de Roles

Grupo de trabajo para la dirección de TIC

- Revisa y, en su caso, aprueba la directriz rectora del proceso de Administración de riesgos de TIC.

Titular de la UTIC

- Integra el Grupo de Trabajo de Riesgos de TIC.

Grupos de trabajo de riesgos de TIC

- Realiza las actividades contenidas en el proceso.

5.2.2.3 indicadores

	INDICADOR
NOMBRE	Cumplimiento de la administración de riesgos de TIC
OBJETIVO	Obtener la efectividad del proceso
DESCRIPCIÓN	Conocer el cumplimiento del proceso por la medición de la implantación de las directrices rectoras del proceso
DIMENCIÓN	Efectividad
TIPO	De gestión

FORMULA	% de efectividad= (Directrices de administración de riesgos de TIC implantadas)/(Directrices de la administración de riesgos de TIC planeadas)*100
RESPONSABLE	Grupo de trabajo de riesgos de TIC
FRECUENCIA DE CÁLCULO	Semestral

5.9.4.4 Reglas del Proceso

1. El titular de la UTIC asignará a los servidores públicos que se encuentran adscritos a la UTIC, los roles que deberán desempeñar en este proceso, así como al responsable de la adscripción del proceso.

2. La UTIC, a través del Grupo de trabajo de riesgos de TIC, establecerá las directrices para la administración de riesgos de UTIC de la institución.

3. El Grupo de trabajo de la TIC será responsable de este proceso.

4. Serán extensivas a este a este proceso las disposiciones de seguridad de la información establecidas por medio del SGSI.

5. La evaluación de este proceso, deberá realizarse de acuerdo a lo establecido en el proceso de administración de la evaluación de TIC.

6. El grupo de trabajo de riesgos de TIC deberá definir los roles y responsabilidades de los servidores públicos que intervendrán en los programas definidos en este proceso, siguiendo el proceso de establecimiento del modelo de gobernabilidad de TIC.

7. El grupo de trabajo de riesgos de TIC deberá establecer, mediante, la directriz rectora del proceso de administración de riesgos de TIC, los reportes de la gestión de este proceso.

8. La UTIC, a través del grupo de trabajo de riesgos de TIC, deberá implementar y mantener actualizados un repositorio en el cual se contendrá la totalidad de la información que se genere a través del presente proceso.

5.9.1.5 Documentación de soporte del proceso
Los anexos señalados en este proceso serán publicados en la siguiente dirección www.maagtic.gob.mx

ANEXO D 5.2.1 ADMINISTRACIÓN DE LA EVALUACIÓN DE TIC.

5.2.1 Administración de la evaluación de TIC

5.2.1.1 Objetivos del proceso

General:

Establecer mecanismos de seguimientos y evaluación, así como acciones de mejora a partir de los resultados de la ejecución, de la planeación estratégica, de la operación de los procesos y de los proyectos, del uso y aprovechamiento de los activos, de los recursos y de la entrega de los servicios TIC.

Específicos

1. Establecer un sistema que permita evaluar en forma integral, o por componentes la operación y servicios de TIC.

2. Proporcionar informes de resultados de la operación y de rendimiento de los procesos y de los servicios de las TIC y de avance en el cumplimiento de los objetivos, que les permita tomar decisiones oportunas e informadas.

3. Establecer las acciones de mejora para proveer y corregir las desviaciones en la operación y rendimiento de los procesos y de los servicios así como dar seguimiento a los resultados de estas acciones.

5.2.1.2 Descripción del proceso

5.2.1.2.1 Descripción de las actividades del proceso

AE-1 Establecer el Sistema para la Evaluación de TIC

Descripción

Establecer los elementos necesarios para instrumentar el sistema que permita dar seguimiento al avance y rendimiento en la implementación de la estrategia y de los proyectos; a la operación y resultados de los procesos; al uso de los recursos, así como a la entrega de los servicios TIC.

Factores Críticos:

El administrador de sistema de evaluación de TIC deberá:

1. Identificar, categorizar, y documentar un conjunto de indicadores de proceso, de producto y de resultados.

2. Verificar el diseño de los indicadores establecidos para cada proceso del “Marco Rector de Procesos en Materia TIC”, de manera que se asegure su constancia e integridad.

   Deben orientarse a:

   - Reducción de costos
   - Cumplimiento regulatorio
   - Satisfacción de los usuarios
   - Madurez y la optimización del proceso
   - Niveles de servicio
   - Cumplimiento de los objetivos estratégicos

3. Actualizar continuamente la información insumo para operar lo indicadores.

4. Formalizar y aprobar el estacionamiento de los indicadores.

5. Considerar al establecer el Sistema de evaluación de TIC, los elementos siguientes:

   - Riesgos de TIC y cumplimiento normativo
   - Niveles de satisfacción de los usuarios
   - Indicadores de operación y resultados de los procesos de TIC

6. Sensibilizar a los servidores públicos de la UTIC y a los usuarios sobre la importancia de la evaluación de TIC.

Relación de productos:

- Anexo 4, Formato 1 “Objetivos e indicadores del sistema de evaluación de TIC”

AE-2 ALINEAR LOS INSUMOS Y LAS MÉTRICAS

Descripción:

Alinear las métricas y la información que sirve de insumo, de acuerdo a la operación de la UTIC, con estricto apego a los indicadores de los procesos del “Marco Rector de Procesos en Materia de TIC”.

Factores Críticos:

El administrador de métricas deberá de:

1. Identificar las métricas de los indicadores

2. Establecer los nombres, categorías, unidades de medida, entre otros atributos de las propias métricas

3. Especificar los métodos o fórmulas de cálculo de las métricas
   Revisar, aprobar y formalizar las métricas

4. Verificar la prioridad y vigencia de las métricas periódicamente

Relación de productos

- Anexo 4, Formato 1 “Objetivos e indicadores del sistema de evaluación de TIC”

AE-3 Especificar los mecanismos de recolección y almacenamiento

Descripción

Especificar cómo son obtenidos y almacenados los datos de las métricas.

Factores Críticos

El administrador de métricas deberá de:

1. Identificar orígenes de datos.

2. Identificar métricas para las cuales se requieren datos que no se encuentran disponibles y, en su caso, revisar la definición de la métrica.

3. Especificar como recolectar y almacenar datos para cada métrica requerida.

4. Crear mecanismos y una guía para la recolección y almacenamiento de datos, integrados en los procesos a medir.

5. Establecer sistemas y mecanismos para la recolección automática de datos cuando sea apropiado y viable.

6. Priorizar, revisar, aprobar y formalizar tanto las métricas como los mecanismos de recolección y almacenamiento de datos.

7. Actualizar métricas e indicadores periódicamente.

Relación de productos:

- Anexo 4, Formato 3 “Mecanismos de Recolección y Almacenamiento de Datos”
- Herramientas de Recolección y almacenamiento de datos

AE-4 Especificar los métodos de análisis

Descripción:

Especificar los métodos para el análisis y reporte de los datos del sistema de evaluación de TIC.

Factores Críticos:

El administrador de métricas deberá de:

1. Especificar y priorizar los análisis de información y los reportes.

2. Seleccionar métodos y herramientas apropiados para el análisis de datos.

3. Revisar y actualizar el contenido y el formato de los informes para realizar los análisis especificados.

4. Especificar los criterios para evaluar la utilidad de los resultados y de las actividades de medición y análisis.

5. Efectuar, anualmente, una verificación sobre las métricas, indicadores y criterios para evaluar los resultados del análisis y, en su caso, actualizar las métricas, indicadores y criterios.

Relación de productos:

- Métodos de análisis del sistema de evaluación de TIC
- Herramienta de análisis de datos

AE-5 Establecer el repositorio de métricas

Descripción

Establecer y mantener actualizado el repositorio de métricas del sistema de evaluación de TIC.

Factores Críticos

El repositorio de métricas deberá ser diseñado como un componente del sistema de conocimiento de acuerdo al proceso de administración del conocimiento y contendrá la información necesaria para entender, interpretar y evaluar las métricas, así como la referencia hacia otra información relacionada.

El administrador del sistema de evaluación de TIC deberá:

1. Determinar las necesidades de almacenamiento y recuperación de métricas.

2. Diseñar e implementar el repositorio de métricas.

3. Especificar los procedimientos para almacenar, actualizar y recuperar las métricas.

4. Mantener disponible para su uso el contenido del repositorio de métricas.

5. Revisar periódicamente, el repositorio de métricas y los mecanismos.

Relación de productos:

- Repositorio de métricas.

AE-6 Recolectar y revisar los datos de insumo para las métricas

Descripción

Obtener los datos de insumo para las métricas y analizar e interpretar los mismos.

Factores Críticos

El analista de evaluación de TIC deberá:

1. Obtener y/o generar los datos de insumo para las métricas.

2. Revisar los datos de insumo para las métricas y verificar su integridad y exactitud.

3. Almacenar la información de acuerdo con los mecanismos de almacenamiento de datos para las métricas.

4. Efectuar periódicamente la actualización de los criterios de revisión.

Relación de productos

- Anexo 4, Formato 4 “Reportes de Resultados Obtenidos en la revisión”

AE-7 Elaborar informes de medición y análisis

Descripción

Elaborar los informes de medición y análisis de la estrategia y de los proyectos; de la operación y resultados de los procesos; del uso de los recursos, así como de la entrega de los servicios TIC.

Factores Críticos

El analista de evaluación de TIC deberá:

1. Elaborar los informes de manera que cumplan con los criterios de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

    - Los informes deberán de ser diseñados para mostrar aquellos asuntos y riesgos relacionados con la contribución de TIC, particularmente con la capacidad de desarrollo de soluciones tecnológicas y la entrega de servicios de TIC, así como con el grado de cumplimiento de los objetivos de los procesos.

2. Desarrollar un análisis inicial de los datos de insumo para las métricas, interpretar los resultados y desarrollar las conclusiones preliminares.

3. Revisar las conclusiones preliminares.

4. Desarrollar, en su caso, análisis complementarios de datos de insumo adicionales para las métricas y preparar los resultados, cuando así proceda, para su presentación.

5. Asesorar a los grupos de trabajo involucrados respecto a esta actividad.

Relación de productos

- Anexo 4, Formato 5 “Informes de Medición y Análisis”

AE-8 Comunicar al Grupo de trabajo para la dirección de TIC y a los servidores públicos involucrados.

Descripción

- Mantener informado a los grupos de trabajo involucrados con respecto a los resultados de la medición y análisis de la estrategia y de los proyectos; de la operación y resultados de los procesos; del uso de los recursos, así como la entrega de los servicios de TIC.

Factores Críticos

El administrador del sistema de evaluación de TIC deberá:

1. Consolidar los resultados de los informes de medición y análisis en informes ejecutivos que reflejen el impacto en la operación de la institución (positivo o negativo).

2. Establecer un mecanismo para dar a conocer, en forma oportuna y confiable los informes ejecutivos.

3. Informar, en su caso las acciones que se realizaron para mitigar aquellos riesgos que fueron identificados.

Relación de productos:

- Anexo 4, Formato 6 “informes Ejecutivos de Evaluación de TIC”.

AE-9 Implementar Acciones de Mejora

Descripción

Identificar desviaciones, problemas y oportunidades de mejora con base en los informes de medición y análisis, para definir e implementar las acciones correctivas y preventivas.

Factores Críticos

El analista de evaluación de TIC deberá:

1. Identificar desviaciones, problemas y oportunidades de mejora con base en los informes de medición y análisis.

2. Determinar las acciones correctivas y preventivas a fin de establecer el programa de mejora, incorporando en el mismo aquéllas actividades de revisiones periódicas.

3. Efectuar negociaciones con los servidores públicos involucrados en los procesos del “Marco Rector de Procesos en Materia de TIC”, para implementar el Programa de Mejora.

4. Definir los resultados esperados de la implementación del Programa de Mejora.

5. Ejecutar el Programa de Mejora.

6. Evaluar los resultados de los programas de mejora, incluyendo la identificación de sus desviaciones.

Relación de Productos

- Anexo 4, Formato “Programa de Mejora”

Tiempo Total del Proceso: *VARIABLE*

5.2.1.2.2 Mapa General de Proceso

Diagrama de flujo de información

Se encuentra disponible en la siguiente dirección: www.maagtic.gob.mx

Diagrama de flujo de actividades

Se encuentra disponible en la siguiente dirección: www.maagtic.gob.mx

5.2.1.2.3 Descripción de Roles

Administración de métricas:

- Especificar los métodos de análisis.
- Alinear los insumos y las métricas.

Administrador del sistema de evaluación de TIC:

- Establecer el sistema para la evaluación de TIC.
- Establecer el repositorio de métricas.
- Comunicar al Grupo de trabajo para la dirección de TIC y a los servidores públicos involucrados.

Analista de evaluación de TIC:

- Recolectar y revisar los datos de insumo para las métricas.
- Elaborar informes de medición y análisis.
- Implementar acciones de mejora.

5.2.1.3 Indicadores

	INDICADOR
NOMBRE	Resultados del Sistema de evaluación de TIC.
OBJETIVO	Conocer la eficacia con la que está operando el Sistema de evaluación de TIC.
DESCRIPCIÓN	Medir los problemas resueltos, identificados por medio del Sistema de evaluación de TIC.
DIMENCIÓN	Eficacia
TIPO	De gestión
FORMULA	% de eficacia= (Problemas resueltos)/(Problemas identificados por medio del sistema de evaluación de TIC)*100
RESPONSABLE	Administrador de métricas
FRECUENCIA DE CÁLCULO	Semestral

5.9.4.4 Reglas del Proceso

1. El titular de la UTIC asignará a los servidores públicos que se encuentran adscritos a la UTIC, los roles que deberán desempeñar en este proceso, así como al que será responsable de la administración de este proceso.

2. La UTIC designará al Administrador de métricas el cual se deberá asegurar de que la instrumentación y operación del sistema de evaluación de TIC se integre conforme al presente proceso.

3. La UTIC, a través del Administrador de métricas, deberá considerar en el diseño del Sistema de evaluación de TIC los requerimientos de datos e información para el análisis de la aplicación de los procesos del “Marco Rector de Procesos en Materia de TIC”.

4. La UTIC, a través del Administrador de métricas, se deberá asegurar de que el Sistema d evaluación de TIC sea consistente con los sistemas de evaluación de la Institución.

5. Serán extensivas a este proceso las disposiciones de seguridad de la información establecidas por medio del SGSI.

6. La evaluación de este proceso, deberá realizarse de acuerdo a lo establecido en el proceso de Administración de la evaluación de TIC.

7. Los roles y responsabilidades de este proceso deberán definirse mediante el proceso de Establecimiento del modelo de gobernabilidad de TIC.

8. La UTIC, a través el Administrador de métricas, deberá implementar y mantener actualizado un repositorio en el cual se contendrá la totalidad de la información que se genere a través del presente proceso.

5.2.1.5 Documentación de soporte del proceso

Los anexos señalados en este proceso serán publicados en la dirección siguiente:
www.maagtic.gob.mx

C A P I T U L O 3

RESULTADOS Y SOLUCIONES DADOS POR EL SGSI

Análisis externo de Vulnerabilidades

Reporte Ejecutivo. Análisis de Vulnerabilidades

Introducción

Este reporte está enfocado plenamente a la detección de vulnerabilidades por lo que los resultados obtenidos deberán ser utilizados para generar un análisis de impacto que permita visualizar el riesgo real para los activos analizados y la información que manejan.

Objetivo

El análisis de vulnerabilidades se orienta a:

- Identificar y analizar cualquier tipo de vulnerabilidad en los activos analizados.
- Orientar al cliente para la mitigación de estas.
- Ofrecer continuidad en el seguimiento de acciones de mitigación.

Herramientas y Técnicas

Los **consultores de resultados** se basan en metodologías de prueba que han sido revisadas y avaladas por la comunidad de seguridad informática para determinar si la red del **organismo receptor** es susceptible de sufrir un ataque informático. Estas prácticas y técnicas de prueba han sido desarrolladas y refinadas constantemente para representar las principales amenazas a las que se encuentra expuesta una empresa con presencia en Internet actualmente.

Los **consultores de resultados** utilizan diversos productos de escaneo que son reconocidos como estándares de la industria, como Outpost24 Líder de tecnología en la evaluación de la vulnerabilidad y manejo de redes, Acunetix, Nessus, N-Stealth, Wikto y otros. Se utilizan diversos programas de escaneo de distintos proveedores con el fin de evitar que los resultados estén sesgados o restringidos a la visión de un solo proveedor. Adicionalmente a los programas de escaneo también se utiliza una variedad de herramientas reconocidas como estándares en la industria tales como, NMAP, SAM Spade, Solarwinds, hping2, metasploit, hydra, l0phtcrack, john-the-ripper, brutus, psexec y muchas otras hechas por profesionales de seguridad para profesionales de seguridad. Los **consultores de resultados** han desarrollado técnicas, scripts y programas en casa que se combinan con los programas anteriormente enumerados para aumentar el alcance y velocidad de la prueba.

Al realizar las pruebas de penetración los **consultores de resultados** asumen el papel de atacantes tomando los principios y actitudes mentales que los atacantes utilizan como pensar “outside of the box”. Los servicios de prueba de penetración de los **consultores de resultados** tienen su base en “Open Source Security Testing Methodology Manual” una metodología aprobada y publicada por ISECOM.

Alcance

Analizar específicamente los activos citados a continuación:

148.***.***.**1	148.***.***.**3	148.***.***.**7
148.***.***.**2	148.***.***.**4	148.***.***.**8
148.***.***.1	148.***.***.6	148.***.***.**9
148.***.***.2	148.***.***.**5	148.***.***.*1
148.***.***.4	148.***.***.**6	148.***.***.*2
148.***.***.5	148.***.***.*3	200.***.***.*1

Análisis de Vulnerabilidades

Durante el análisis realizado a los 18 activos proporcionado por el departamento de Sistemas del **organismo receptor**, fue posible detectar un número considerable de vulnerabilidades. El análisis arrojó las siguientes vulnerabilidades:

Host	Nombre	Alto impacto	Mediano impacto	Bajo impacto	Total de vulnerabilidades	Puertos
148.*.***.**1**	mail2.********.gob.mx	0	2	0	2	2
148.*.***.**2**	**********.********.gob.mx	0	2	0	2	1
148.*.***.**3**	na-148-***-***-***.******.*******.net.mx	0	1	0	1	2
148.*.***.**4**	na-148-***-***-***.******.*******.net.mx	0	0	0	0	1
148.*.***.**7**	na-148-***-***-***.******.*******.net.mx	0	2	0	2	1
148.*.***.**8**	*****001.********.gob.mx	1	7	1	9	5
148.*.***.1**	*********.*****.com	0	1	0	1	5
148.*.***.2**	na-191-2.******.*******.net.mx	0	0	0	0	1
148.*.***.4**	na-191-4.******.*******.net.mx	0	1	0	1	4
148.*.***.5**	na-191-5.******.*******.net.mx	0	0	0	0	1
148.*.***.6**	na-191-6.******.*******.net.mx	0	1	1	2	12
148.*.***.**5**	evaluaciones.********.gob.mx	0	4	1	5	3
148.*.***.**6**	********.mx	1	5	1	7	2
148.*.***.*3**	proyectos.********.gob.mx	0	7	2	9	2
148.*.***.**9**	********.gob.mx	1	0	1	2	2
148.*.***.*1**	********qa1.********.gob.mx	0	4	0	4	1
148.*.***.*2**	prod.********.gob.mx	0	2	0	2	2
200.*.***.*1**	cust-200-**-***-**.*****.com	0	0	0	0	3

Las vulnerabilidades marcadas como **impacto alto** son aquellas que pueden causar mayor impacto al ser explotadas, pudiéndose llevar a cabo actividades riesgosas que pongan en peligro la integridad, confidencialidad o disponibilidad del activo en el que se ejecute dicha vulnerabilidad. Por ejemplo, actividades como: denegación de servicio, acceso no autorizado, publicación de información confidencial, suplantación de identidad, etc.
Las vulnerabilidades marcadas como **impacto medio** son aquellas que pueden no representar un riesgo alto aun que estas puedan afectar la integridad, confidencialidad o disponibilidad de los activos.
Las vulnerabilidades marcadas como **impacto bajo** son aquellas que no causan un alto impacto en los servicios de los activos.

Top de Vulnerabilidades

Los activos categorizados como críticos por el **organismo receptor** cuentan actualmente con las siguientes vulnerabilidades, las cuales se presentan en mayor cantidad

Vulnerabilidad	Activo	Riesgo	Mitigación
Cross site scripting (XSS)	148.***.***.**6	Permite Usuarios malintencionados inyectar JavaScript, VBScript, ActiveX, HTML o Destellar en un uso vulnerable para engañar a un usuario para juntar datos de ellos. Un atacante puede robar las cookies de sesión y asumir la cuenta, imitando al usuario. Es también posible modificar el contenido que se le presenta al usuario.	Validar los datos de entra que se introducen
SQL INJECTION	148.***.***.**9	Permite a un atacante alterar sentencias SQL mediante la manipulación de la entrada del usuario. Una inyección SQL sucede cuando las aplicaciones web, aceptar la entrada de usuario que se depositen directamente en una sentencia SQL y no filtrar correctamente los caracteres.	Validar los datos de entra que se introducen
Métodos HTTP soportados DELETE, GET, PUT, TRACE	DELETE, GET,PUT 148.***.***.**8, TRACE, 148.***.***.**8 148.***.***.**6 148.***.***.*3 148.***.***.**5 148.***.***.*2 148.***.***.*1	Un atacante puede usar estos métodos para modificar, borrar y tomar control de activo	Deshabilitar estos métodos.
Múltiples vulnerabilidades en la versión de Microsoft IIS	148.***.***.**6 148.***.***.*3 148.***.***.**5 148.***.***.**8	Un atacante podría aprovechar este problema para realizar ataques Man-in-the-middle, creación de archivos vía remota	Actualizar a la última versión estable
Autenticación en texto claro (Telnet)	148.***.***.1	Podría permitir a un atacante captar la información de usuario y Password, ganando accesos al equipo y tomar el control del activo	Migrar a SSH y/o filtrar accesos
DNS recursive queries	148.***.***.**3	Cualquier persona puede solicitar una búsqueda de cualquier nombre de dominio. Un atacante puede aprovechar este problema para realizar ataques de envenenamiento de caché contra este servidor de nombres. Si el DNS permite consultas recursivas a través de UDP, esta máquina puede, potencialmente, ser utilizada para 'rebotar' ataques de denegación de servicio contra otras redes o sistemas.	Restringir las consultas recursivas a los anfitriones que debe utilizar este servidor de nombres, como los de la LAN conectados a él.

Múltiples vulnerabilidades en la versión SSL/TLS	148.***.***.6 148.***.***.**1 148.***.***.**2 148.***.***.**8 148.***.***.**7	Las versiones obsoletas y/o el cifrado débil podrían permitir a un atacante escuchar disimuladamente sobre la comunicación que viaja en la red.	Establecer contraseñas robustas en la autenticación y endurecer el tipo de cifrado así como actualizar la versión de SSL a la versión 3

.

Servicios vulnerables

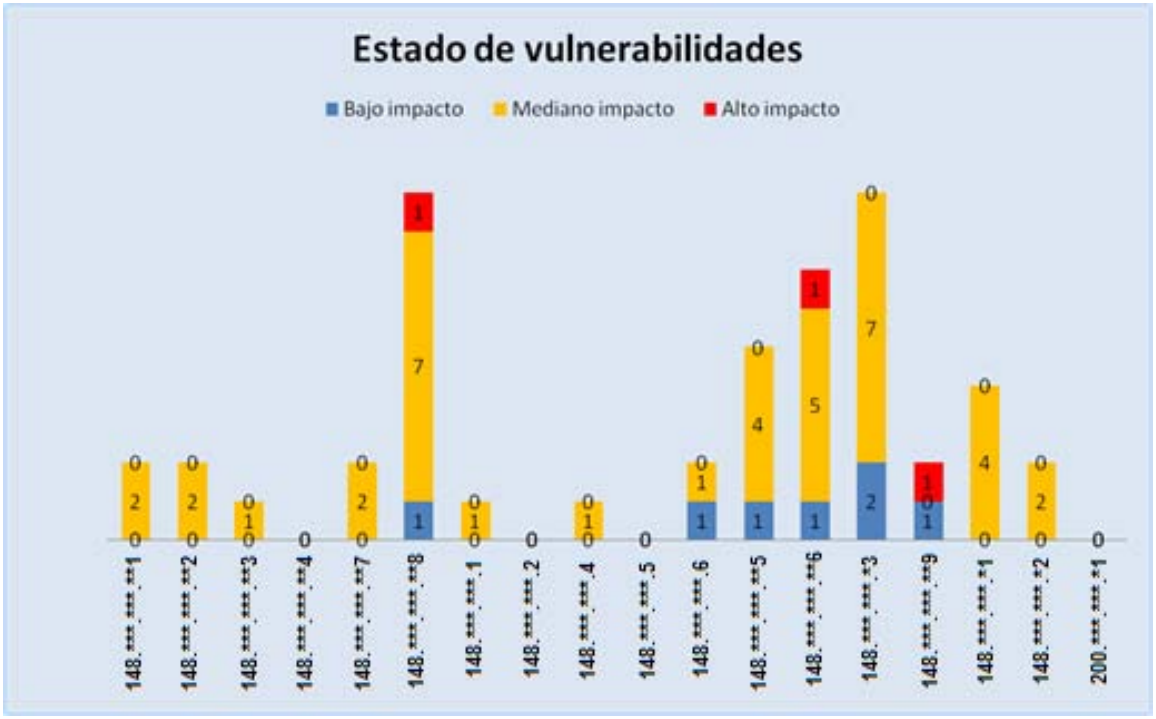
Los activos analizados cuentan actualmente con servicios vulnerables.

Servicio	Puerto	Descripción
SSL / TLS	80 443	Puede ser vulnerable si es que dicho servicio contase con una versión obsoleta de los certificados del servicio, ya que proporcionaría accesos débiles para la autenticación.
telnet	23	Podría ser aprovechado para que un atacante capturara usuario y Password ya que viaja en texto claro.
Ssh	22	Podría ser aprovechado para que un atacante ejecutara ataques de denegación de servicio e incluso, según el advisory original, ejecutar código arbitrario
HTTP	80	Puede ser un servicio vulnerable porque mediante ese servicio son mandados mensajes que contienen información crítica del sistema, podría permitir a un usuario malintencionado provocar negación de servicios y/o ejecutar código arbitrario en forma remota
DNS	53	Cualquier persona puede solicitar una búsqueda de cualquier nombre de dominio. Un atacante puede aprovechar este problema para realizar ataques de envenenamiento de caché contra este servidor de nombres.

Estado de vulnerabilidades

En la siguiente gráfica se muestran los índices de vulnerabilidades de acuerdo al nivel de impacto para cada uno de los activos.

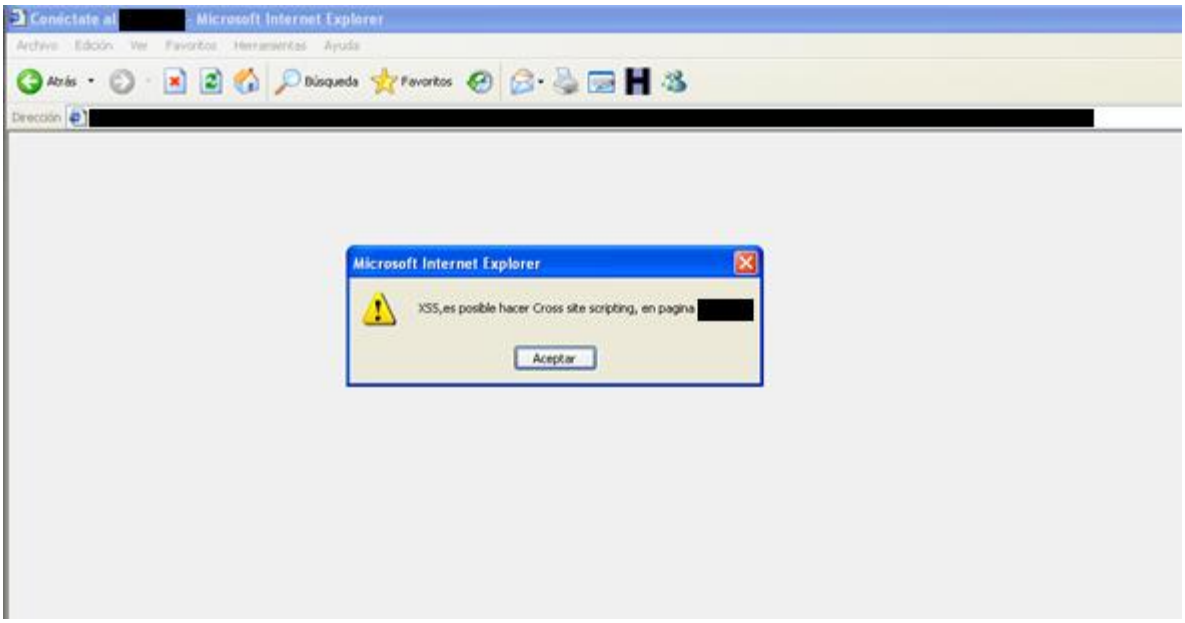
Índice de vulnerabilidades por activo



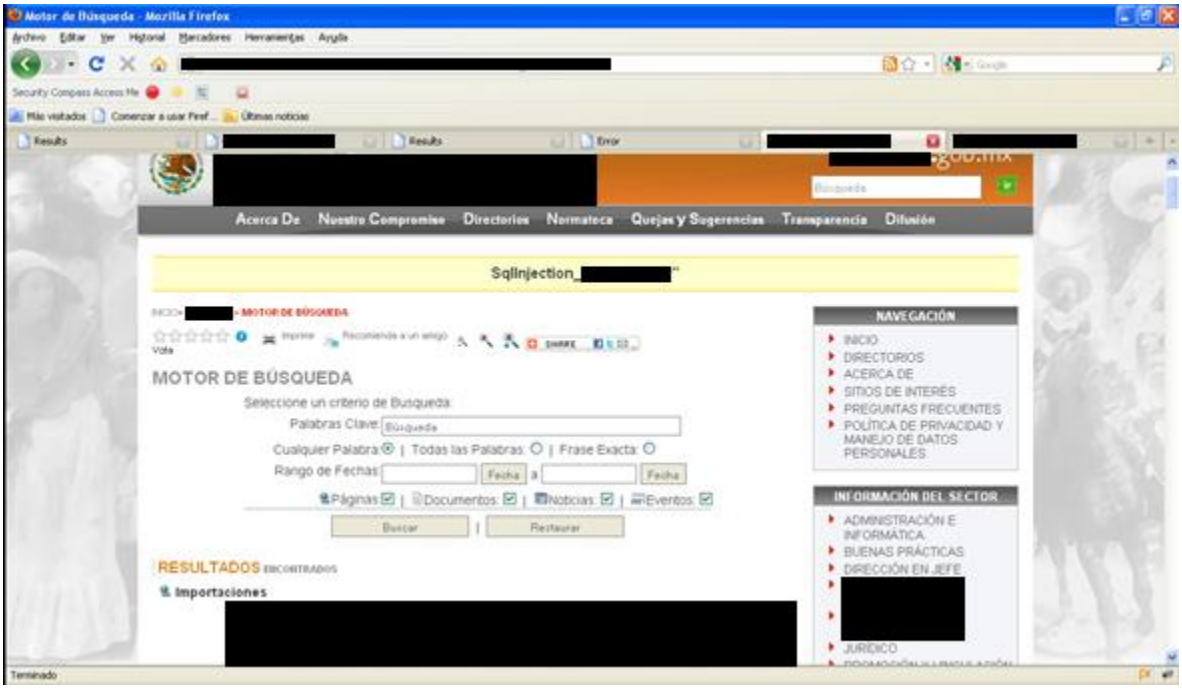
Evidencia de vulnerabilidades

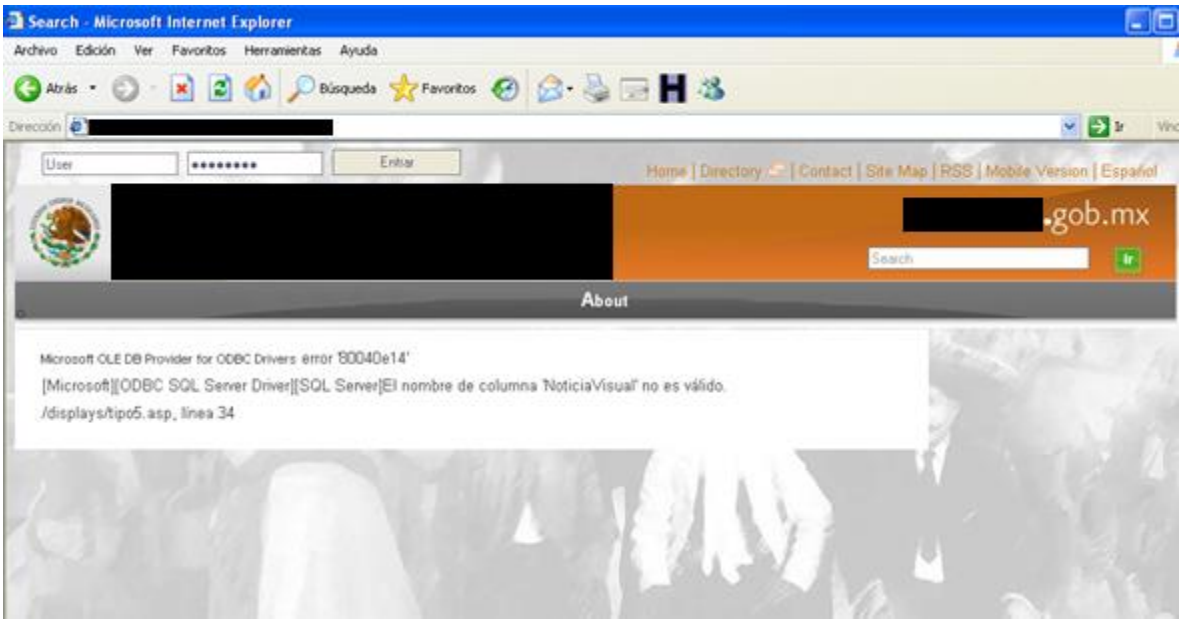
Mediante las comprobaciones manuales realizadas a los activos, se pudo detectar ciertas vulnerabilidades. Por mencionar algunas.

Cross Site Scripting XSS

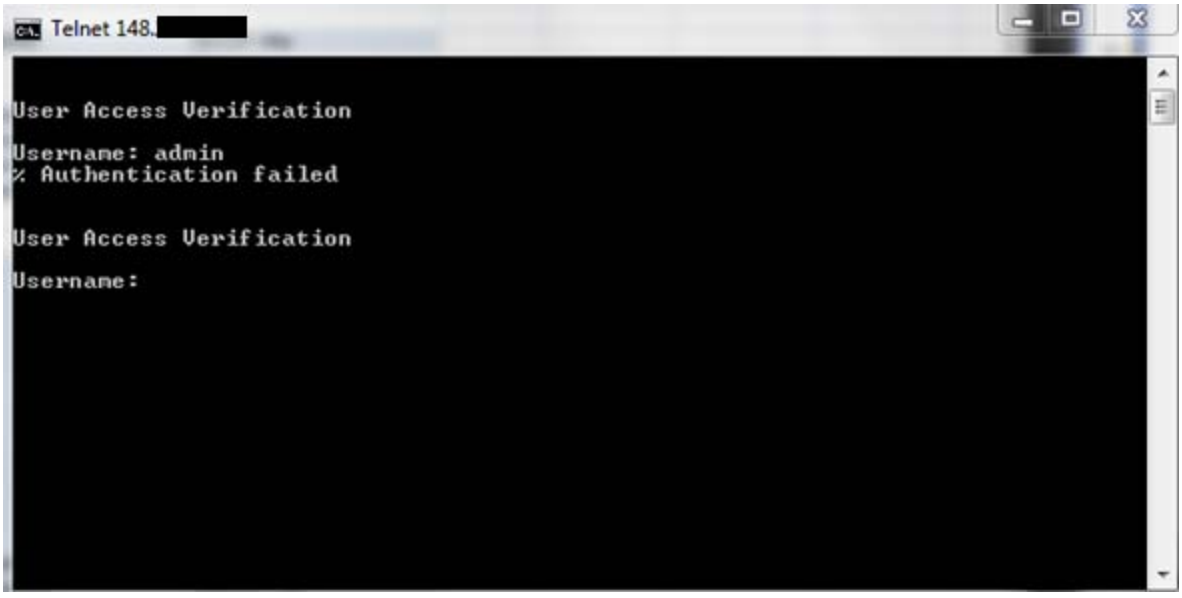


SQL Injection

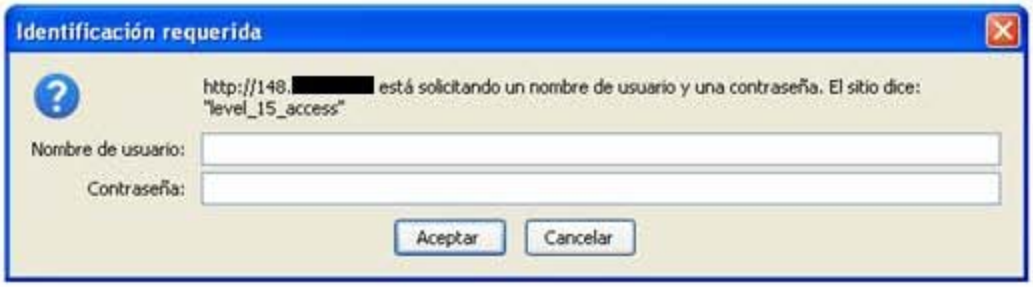




Administración en texto claro Telnet y administración de equipos de red vía web




```
401 Unauthorized
```



Anexo

Detalle técnico de cada uno de los activos.

Host	Vulnerabilidad	Puerto	Factor de Impacto	Descripción	Información	Solución	Referencia	CVE
148.*.***.**6**	Cross Site Scripting	80	Alto	Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.	Affected items /	Your script should filter metacharacters from user input.		

148.*.***.**9**	SQL injection	80	Alto	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter backend SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.	Affected items /	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.		
148.*.***.**8**	HTTP Options Supported	443	Alto	The following options are supported by the web server running on this port.	OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH			

148.*.***.**6**	Microsoft IIS TLS Renogotiation Man-in-the-middle Vulnerability	80	**Medio**	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.	This vulnerability was identified because (1) the version of Microsoft IIS is 6.0. Paths: /	Upgrade to the latest version of Microsoft IIS.	url - http://www.iis.net/ solution - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555	CVE-2009-3555

148.*.***.**6**	Microsoft IIS: ASP Crafted semicolon Extension Security Bypass	80	**Medio**	Microsoft Internet Information Services (IIS) 5.x and 6.x uses only the portion of a filename before a ; (semicolon) character to determine the file extension, which allows remote attackers to bypass intended extension restrictions of third-party upload applications via a filename with a (1) .asp, (2) .cer, or (3) .asa first extension, followed by a semicolon and a safe extension, as demonstrated by the use of asp.dll to handle a .asp;.jpg file	This vulnerability was identified because (1) the version of Microsoft IIS is 6.0. Paths: /	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.iis.net/	CVE-2009-4444

148.*.***.**6**	Microsoft IIS: Colon Safe Extension NTFS ADS Filename Syntax Arbitrary Remote File Creation	80	**Medio**	Microsoft Internet Information Services (IIS), when used in conjunction with unspecified third-party upload applications, allows remote attackers to create empty files with arbitrary extensions via a filename containing an initial extension followed by a: (colon) and a safe extension, as demonstrated by an upload of a .asp:.jpg file that results in creation of an empty .asp file, related to support for the NTFS Alternate Data Streams (ADS) filename syntax. NOTE: it could be argued that this is a vulnerability in the third-party product, not IIS, because the third-party product should be applying its extension restrictions to the portion of the filename before the colon.	This vulnerability was identified because (1) the version of Microsoft IIS is 6.0.Paths: /	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.iis.net/	CVE-2009-4445

148.*.***.**6**	HTTP TRACE/TRACK Cross-Site Scripting Attack	80	**Medio**	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "cross-site tracing", when used in conjunction with various weaknesses in browsers. This is related to CVE-2004-2320 and CVE-2005-3398	Service responded to a TRACE request with the status code 200 and included our forged headers in the response	If the remote host is running Microsoft IIS, Use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. If the remote host is running Apache HTTP Daemon, Add the following lines for each virtual host in your configuration file: RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F]	solution - http://www.microsoft.com/technet/security/tools/urlscan.mspx solution - http://learn.iis.net/page.aspx/938/urlscan-3-reference/#UsingUrlScan	CVE-2007-3008

148.*.***.**6**	IIS Auth	80	**Medio**	Information leaks in IIS 4 through 5.1 allow remote attackers to obtain potentially sensitive information or more easily conduct brute force attacks via responses from the server in which (1) the server reveals whether it supports Basic or NTLM authentication through 401 Access Denied error messages, (2) in certain configurations, the server IP address is provided as the realm for Basic authentication, which could reveal real IP addresses that were obscured by NAT, or (3) when NTLM authentication is used, the NetBIOS name of the server and its Windows NT domain are revealed in response to an Authorization request.	This vulnerability was identified because (1) an installation of Microsoft IIS was found; and (2) it was possible to gain access to unintended information through the file '//'. Paths: /	Currently no available solution.	url - http://www.nextgenss.com/advisories/iisauth.txt	CVE-2002-0419

148.*.***.*3**	Microsoft IIS TLS Renogotiation Man-in-the-middle Vulnerability	80	**Medio**	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.	This vulnerability was identified because (1) the version of Microsoft IIS is 6.0.Paths: /	Upgrade to the latest version of Microsoft IIS.	url - http://www.iis.net/solution - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555	CVE-2009-3555

148.*.***.*3**	Microsoft IIS TLS Renogotiation Man-in-the-middle Vulnerability	9001	**Medio**	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.	This vulnerability was identified because (1) the version of Microsoft IIS is 6.0. Paths: /	Upgrade to the latest version of Microsoft IIS.	url - http://www.iis.net/ solution - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555	CVE-2009-3555

148.*.***.*3**	Microsoft IIS: ASP Crafted semicolon Extension Security Bypass	80	**Medio**	Microsoft Internet Information Services (IIS) 5.x and 6.x uses only the portion of a filename before a ; (semicolon) character to determine the file extension, which allows remote attackers to bypass intended extension restrictions of third-party upload applications via a filename with a (1) .asp, (2) .cer, or (3) .asa first extension, followed by a semicolon and a safe extension, as demonstrated by the use of asp.dll to handle a .asp;.jpg file.	This vulnerability was identified because (1) the version of Microsoft IIS is 6.0. Paths: /	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.iis.net/	CVE-2009-4444
148.*.***.*3**	Microsoft IIS: ASP Crafted semicolon Extension Security Bypass	9001	**Medio**	Microsoft Internet Information Services (IIS) 5.x and 6.x uses only the portion of a filename before a ; (semicolon) character to determine the file extension, which allows remote attackers to bypass intended extension restrictions of third-party upload applications via a filename with a (1) .asp, (2) .cer, or (3) .asa first extension, followed by a semicolon and a safe extension, as demonstrated by the use of asp.dll to handle a .asp;.jpg file.	This vulnerability was identified because (1) the version of Microsoft IIS is 6.0. Paths: /	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.iis.net/	CVE-2009-4444

148.*.***.*3**	Microsoft IIS: Colon Safe Extension NTFS ADS Filename Syntax Arbitrary Remote File Creation	80	**Medio**	Microsoft Internet Information Services (IIS), when used in conjunction with unspecified third-party upload applications, allows remote attackers to create empty files with arbitrary extensions via a filename containing an initial extension followed by a : (colon) and a safe extension, as demonstrated by an upload of a .asp:.jpg file that results in creation of an empty .asp file, related to support for the NTFS Alternate Data Streams (ADS) filename syntax. NOTE: it could be argued that this is a vulnerability in the third-party product, not IIS, because the third-party product should be applying its extension restrictions to the portion of the filename before the colon.	This vulnerability was identified because (1) the version of Microsoft IIS is 6.0.Paths: /	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.iis.net/	CVE-2009-4445

148.*.***.*3**	Microsoft IIS: Colon Safe Extension NTFS ADS Filename Syntax Arbitrary Remote File Creation	9001	**Medio**	Microsoft Internet Information Services (IIS), when used in conjunction with unspecified third-party upload applications, allows remote attackers to create empty files with arbitrary extensions via a filename containing an initial extension followed by a : (colon) and a safe extension, as demonstrated by an upload of a .asp:.jpg file that results in creation of an empty .asp file, related to support for the NTFS Alternate Data Streams (ADS) filename syntax. NOTE: it could be argued that this is a vulnerability in the third-party product, not IIS, because the third-party product should be applying its extension restrictions to the portion of the filename before the colon.	This vulnerability was identified because (1) the version of Microsoft IIS is 6.0. Paths: /	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.iis.net/	CVE-2009-4445

148.*.***.*3**	HTTP TRACE/TRACK Cross-Site Scripting Attack	80	**Medio**	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "cross-site tracing", when used in conjunction with various weaknesses in browsers. This is related to CVE-2004-2320 and CVE-2005-3398	Service responded to a TRACE request with the status code 200 and included our forged headers in the response	If the remote host is running Microsoft IIS, Use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. If the remote host is running Apache HTTP Daemon, Add the following lines for each virtual host in your configuration file: RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F]	solution - http://www.microsoft.com/technet/security/tools/urlscan.mspx solution - http://learn.iis.net/page.aspx/938/urlscan-3-reference/#UsingUrlScan	CVE-2007-3008

148.*.***.**5**	Microsoft IIS TLS Renogotiation Man-in-the-middle Vulnerability	80	**Medio**	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.	This vulnerability was identified because (1) the version of Microsoft IIS is 6.0.Paths: /	Upgrade to the latest version of Microsoft IIS.	url - http://www.iis.net/solution - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555	CVE-2009-3555

148.*.***.**5**	Microsoft IIS: ASP Crafted semicolon Extension Security Bypass	80	**Medio**	Microsoft Internet Information Services (IIS) 5.x and 6.x uses only the portion of a filename before a ; (semicolon) character to determine the file extension, which allows remote attackers to bypass intended extension restrictions of third-party upload applications via a filename with a (1) .asp, (2) .cer, or (3) .asa first extension, followed by a semicolon and a safe extension, as demonstrated by the use of asp.dll to handle a .asp;.jpg file.	This vulnerability was identified because (1) the version of Microsoft IIS is 6.0. Paths: /	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.iis.net/	CVE-2009-4444

148.*.***.**5**	Microsoft IIS: Colon Safe Extension NTFS ADS Filename Syntax Arbitrary Remote File Creation	80	**Medio**	Microsoft Internet Information Services (IIS), when used in conjunction with unspecified third-party upload applications, allows remote attackers to create empty files with arbitrary extensions via a filename containing an initial extension followed by a : (colon) and a safe extension, as demonstrated by an upload of a .asp:.jpg file that results in creation of an empty .asp file, related to support for the NTFS Alternate Data Streams (ADS) filename syntax. NOTE: it could be argued that this is a vulnerability in the third-party product, not IIS, because the third-party product should be applying its extension restrictions to the portion of the filename before the colon.	This vulnerability was identified because (1) the version of Microsoft IIS is 6.0. Paths: /	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.iis.net/	CVE-2009-4445

148.*.***.**5**	HTTP TRACE/TRACK Cross-Site Scripting Attack	80	**Medio**	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "cross-site tracing", when used in conjunction with various weaknesses in browsers. This is related to CVE-2004-2320 and CVE-2005-3398	Service responded to a TRACE request with the status code 200 and included our forged headers in the response	If the remote host is running Microsoft IIS, Use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. If the remote host is running Apache HTTP Daemon, Add the following lines for each virtual host in your configuration file: RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F]	solution - http://www.microsoft.com/technet/security/tools/urlscan.mspx solution - http://learn.iis.net/page.aspx/938/urlscan-3-reference/#UsingUrlScan	CVE-2007-3008

148.*.***.*2**	Apache 2.x version older than 2.2.9	80	**Medio**	low: mod_proxy_balancer CSRF CVE-2007-6420The mod_proxy_balancer provided an administrative interface that could be vulnerable to cross-site request forgery (CSRF) attacks. moderate: mod_proxy_http DoS CVE-2008-2364A flaw was found in the handling of excessive interim responses from an origin server when using mod_proxy_http. A remote attacker could cause a denial of service or high memory usage.	Affected Apache versions (2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0).	Upgrade Apache to the latest version.		

148.*.***.*2**	HTTP TRACE/TRACK Cross-Site Scripting Attack	80	**Medio**	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "cross-site tracing", when used in conjunction with various weaknesses in browsers. This is related to CVE-2004-2320 and CVE-2005-3398	Service responded to a TRACE request with the status code 200 and included our forged headers in the response	If the remote host is running Microsoft IIS, Use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. If the remote host is running Apache HTTP Daemon, Add the following lines for each virtual host in your configuration file: RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F]	solution - http://www.microsoft.com/technet/security/tools/urlscan.mspx solution - http://learn.iis.net/page.aspx/938/urlscan-3-reference/#UsingUrlScan	CVE-2007-3008

148.*.***.*1**	HTTP TRACE/TRACK Cross-Site Scripting Attack	80	**Medio**	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "cross-site tracing", when used in conjunction with various weaknesses in browsers. This is related to CVE-2004-2320 and CVE-2005-3398	Service responded to a TRACE request with the status code 200 and included our forged headers in the response	If the remote host is running Microsoft IIS, Use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. If the remote host is running Apache HTTP Daemon, Add the following lines for each virtual host in your configuration file: RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F]	solution - http://www.microsoft.com/technet/security/tools/urlscan.mspx solution - http://learn.iis.net/page.aspx/938/urlscan-3-reference/#UsingUrlScan	CVE-2007-3008

148.*.***.*1**	Apache 2.x version older than 2.2.9	80	**Medio**	low: mod_proxy_balancer CSRF CVE-2007-6420 The mod_proxy_balancer provided an administrative interface that could be vulnerable to cross-site request forgery (CSRF) attacks. moderate: mod_proxy_http DoS CVE-2008-2364 A flaw was found in the handling of excessive interim responses from an origin server when using mod_proxy_http. A remote attacker could cause a denial of service or high memory usage.	Affected Apache versions (2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0).	Upgrade Apache to the latest version.		
148.*.***.*1**	Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow Vulnerability	80	**Medio**	A stack-based buffer overflow has been reported in the Apache mod_ssl module. This issue would most likely result in a denial of service if triggered, but could theoretically allow for execution of arbitrary code. The issue is not believed to be exploitable to execute arbitrary code on x86 architectures, though this may not be the case with other architectures.		Upgrade mod_ssl to the latest version.		

148.*.***.*1**	Apache Mod_SSL Log Function Format String Vulnerability	80	**Medio**	A format string vulnerability has been found in mod_ssl versions older than 2.8.19. Successful exploitation of this issue will most likely allow an attacker to execute arbitrary code on the affected computer.		Upgrade mod_ssl to the latest version.		
148.*.***.6**	Weak Supported SSL Ciphers Suites	8443	**Medio**	The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.		Reconfigure the affected application if possible to avoid use of weak ciphers.	http://www.openssl.org/docs/apps/ciphers.html	
148.*.***.4**	Source code disclosure	80	**Medio**	Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives. An attacker can gather sensitive information (database connection strings, application logic) by analysing the source code. This information can be used to conduct further attacks.	/tsweb	Remove this file from your website or change its permissions to remove access.		

148.*.***.**1**	SSL 2.0 deprecated protocol	80	**Medio**	The remote service encrypts traffic using an old deprecated protocol with known weaknesses. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.		Disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.		
148.*.***.**1**	SSL weak ciphers	80	**Medio**	The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.	Weak SSL ciphers (SSL2 on port 443): SSL2_CK_RC4_128_EXPORT40_WITH_MD5 - Low strength SSL2_CK_RC2_128_CBC_EXPORT40_WITH_MD5 - Low strength SSL2_CK_DES_64_CBC_WITH_MD5 - Low strength	Reconfigure the affected application to avoid use of weak ciphers.		

148.*.***.**2**	SSL 2.0 deprecated protocol	80	**Medio**	The remote service encrypts traffic using an old deprecated protocol with known weaknesses. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.		Disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.		
148.*.***.**2**	SSL weak ciphers	80	**Medio**	The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.	Weak SSL ciphers (SSL2 on port 443): SSL2_CK_RC4_128_EXPORT40_WITH_MD5 - Low strength SSL2_CK_RC2_128_CBC_EXPORT40_WITH_MD5 - Low strength SSL2_CK_DES_64_CBC_WITH_MD5 - Low strength	Reconfigure the affected application to avoid use of weak ciphers.		

148.*.***.**3**	DNS recursive queries	53	**Medio**	This DNS appears to allow recursive queries (i.e. requests for lookupsof third party names).In other words, anyone may request a lookup of any domain name. An attacker can take advantage of this problem to perform cache poisoning attacks againstthis nameserver.If the DNS allows recursive queries over UDP, this host can potentially alsobe used to 'bounce' denial of service attacks against other networks or systems.Note: If this nameserver is your internal nameserver, and the scan was performedfrom within your network, you may disregard this notice.		Restrict recursive queries to the hosts that should use this nameserver,such as those of the LAN connected to it.If you are using a Microsoft DNS sever, follow the applicable instructionsat the following URL: http://www.eukhost.com/forums/archive/index.php/t-852.htmlIf you are using bind 8, this can be done by using the instruction'allow-recursion' in the 'options' section of your 'named.conf'.If you are using bind 9, you can define a grouping of internal addressesusing the 'acl' command.Then, within the options block, you can explicitly state:allow-recursion { hosts_defined_in_acl }'If you are using another name server, consult its documentation.	url - http://www.subneural.net/files/bind9arm.pdfurl - http://technet2.microsoft.com/WindowsServer/en/library/e1fe9dff-e87b-44ae-ac82-8e76d19d9c371033.mspx	

148.*.***.**8**	Microsoft IIS TLS Renogotiation Man-in-the-middle Vulnerability	443	**Medio**	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.	This vulnerability was identified because (1) the version of Microsoft IIS is 6.0. Paths: /	Upgrade to the latest version of Microsoft IIS.	url - http://www.iis.net/ solution - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555	CVE-2009-3555

148.*.***.**8**	Microsoft IIS: ASP Crafted semicolon Extension Security Bypass	443	**Medio**	Microsoft Internet Information Services (IIS) 5.x and 6.x uses only the portion of a filename before a; (semicolon) character to determine the file extension, which allows remote attackers to bypass intended extension restrictions of third-party upload applications via a filename with a (1) .asp, (2) .cer, or (3) .asa first extension, followed by a semicolon and a safe extension, as demonstrated by the use of asp.dll to handle a .asp;.jpg file.	This vulnerability was identified because (1) the version of Microsoft IIS is 6.0. Paths: /	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.iis.net/	CVE-2009-4444

148.*.***.**8**	Microsoft IIS: Colon Safe Extension NTFS ADS Filename Syntax Arbitrary Remote File Creation	443	**Medio**	Microsoft Internet Information Services (IIS), when used in conjunction with unspecified third-party upload applications, allows remote attackers to create empty files with arbitrary extensions via a filename containing an initial extension followed by a: (colon) and a safe extension, as demonstrated by an upload of a .asp:.jpg file that results in creation of an empty .asp file, related to support for the NTFS Alternate Data Streams (ADS) filename syntax. NOTE: it could be argued that this is a vulnerability in the third-party product, not IIS, because the third-party product should be applying its extension restrictions to the portion of the filename before the colon.	This vulnerability was identified because (1) the version of Microsoft IIS is 6.0.Paths: /	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.iis.net/	CVE-2009-4445

148.*.***.**8**	SSL Certificate Authenticity	443	**Medio**	The certificate presented by this service does not seem to have been issued by a valid Certificate Authority (CA). By having a trusted CA sign your certificate, they certify that you are in fact you. Note: This finding is issued if it is not possible to verify the authenticity of the certificate presented by the service, and is sometimes a result of the service being misconfigured. Any SSLv3/TLSv1 compliant service must present the complete chain of certificates used to sign its own, optionally excluding the root CA certificate. A more detailed reason for why the chain of trust was broken is listed in the table in the information section of this finding.	---------- ---------- -- [depth][country][state][locality][organization][common name][error] ---------- ---------- - [0][MX][Distrito Federal][Mexico][********** **********][correo.*******.gob.mx][unable to get local issuer certificate]	Use a valid Certificate Authority (CA)		

148.*.***.**8**	SSLv2 detected	443	**Medio**	An SSLv2 service is running on this port. Version 2 of the SSL protocol is vulnerable to several attacks and weaknesses The main attacks include a 'cipher downgrade' attack and a truncation 'attack'. The cipher downgrade attacks allows an attacker to force an already established session to use a weaker (easier to crack) cipher than originally negotiated. The truncation attack allows an attacker to stop a connection at an arbitrary point. It should be noted that, specifically, SSLv2 includes many weak ciphers and negotiates the ciphers in clear text.		Configure this service to only allow version 3 of the SSL protocol. Consult your product manual or vendor for information about how this is done.	url - http://www.educatedguesswork.org/movabletype/archives/2005/10/openssl_sslv2_r.html solution - http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslciphersuite solution - http://support.microsoft.com/kb/187498 solution - http://redmine.lighttpd.net/wiki/1/Docs:SSL#PCI-DSS-compliance solution - http://wiki.nginx.org/NginxHttpSslModule#ssl_ciphers	

148.*.***.**8**	SSL/TLS Cipher Suite Detect MD5	443	**Medio**	The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5 in the signature algorithm of an X.509 certificate.	----------[SSLv2 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength]----------[RC4_128_WITH_MD5][RC4-MD5][128][128][medium][RC4_128_EXPORT40_WITH_MD5][EXP-RC4-MD5][128][40][export][RC2_128_CBC_WITH_MD5][RC2-CBC-MD5][128][128][medium][RC2_128_CBC_EXPORT40_WITH_MD5][EXP-RC2-CBC-MD5][128][40][export][DES_64_CBC_WITH_MD5][DES-CBC-MD5][56][56][	Reconfigure the service to disallow the listed cipher suites	url - http://www.kb.cert.org/vuls/id/836068	CVE-2004-2761

					weak][DES_192_EDE3_CBC_WITH_MD5][DES-CBC3-MD5][168][168][strong]----------[SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength]----------[RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export][RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium][RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export]----------			

					[TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength]----------[RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export][RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium][RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][exp			

148.*.***.**8**	SSL/TLS Weak and Export Ciphers Detected	443	**Medio**	The service running on this port allows the use of weak encryption ciphers, which might allow an attacker to eavesdrop on the communication.	---------- ---------- -- [SSLv2 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- ---------- - [RC4_128_EXPORT40_WITH_MD5][EXP-RC4-MD5][128][40][export] [RC2_128_CBC_EXPORT40_WITH_MD5][EXP-RC2-CBC-MD5][128][40][export] [DES_64_CBC_WITH_MD5][DES-CBC-MD5][56][56][weak]	For Apache, add the following line to the configuration file (e.g. httpd.conf): SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM and restart the server. For Microsoft IIS, set the following registry keys to 0: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128 HKEY_LOCAL_MACHIN	url - http://support.microsoft.com/default.aspx?scid=kb;en-us;245030 url - http://blog.stardothosting.com/2009/05/22/testing-for-weak-ssl-ciphers-for-security-audits/ url - http://www.routerzone.eu/wiki/index.php/Restricting_Weak_SSL_Ciphers,_F5_BigIP url - http://www.openssl.org/docs/apps/ciphers.html solution - http://blog.zenone.org/2009/03/pci-compliance-disable-	

					---------- ---------- - [SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- ---------- - [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export] [RSA_WITH_DES_CBC_SHA][DES-CBC-SHA][56][56][weak] [RSA_EXPOR	E\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128	sslv2-and-weak.html	

					T1024_WITH_DES_CBC_SHA][EXP1024-DES-CBC-SHA][56][56][export] [RSA_EXPORT1024_WITH_RC4_56_SHA][EXP1024-RC4-SHA][128][56][export] --- [TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] --- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-			

					MD5][128][40][export][RSA_WITH_DES_CBC_SHA][DES-CBC-SHA][56][56][weak][RSA_EXPORT1024_WITH_DES_CBC_SHA][EXP1024-DES-CBC-SHA][56][56][export][RSA_EXPORT1024_WITH_RC4_56_SHA][EXP1024-RC4-SHA][128][56][export]			

148.*.***.1**	Telnet service running	23	**Medio**	The rlogin service is running on this host. Telnet allows users to log in on another host via a network, as if they were physically present at the computer. All information, including passwords, is transmitted unencrypted (making it vulnerable to interception).		If you are not using this service, it is recommended to disable it. Otherwise, replace it with SSH.		
148.*.***.**7**	SSL Certificate Authenticity	443	**Medio**	The certificate presented by this service does not seem to have beenissued by a valid Certificate Authority (CA). By having a trusted CAsign your certificate, they certify that you are in fact you.Note: This finding is issued if it is not possible to verify the authenticityof the certificate presented by the service, and is sometimes a result of theservice being misconfigured. Any SSLv3/TLSv1 compliant service must presentthe complete chain of certificates used to sign its own, optionally excluding the root CA certificate. A more detailed reason for why the chain of trustwas broken is listed in the table in the information section of this finding.	----------[depth][country][state][locality][organization][common name][error]----------[0][][][][][148.***.***.**7][self signed certificate]	Use a valid Certificate Authority (CA)		

148.*.***.**7**	SSL/TLS Renegotiation Handshakes Man-in-the-Middle Plaintext Data Injection	443	**Medio**	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS), mod_ssl in the Apache HTTP Server, OpenSSL, Mozilla Network Security Services (NSS), multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context.		OpenSSL has provided a fix for this in version 0.9.8m and later. Microsoft has released a workaround to disable renegotiation.	solution - http://www.openssl.org/source/ solution - http://support.microsoft.com/kb/977377 solution - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555	CVE-2009-3555

148.*.***.**6**	Microsoft IIS: Crafted DNS Response Inverse Lookup Log Corruption XSS	80	**Bajo**	Microsoft Internet Information Services (IIS) 6.0, when DNS resolution is enabled for client IP addresses, allows remote attackers to inject arbitrary text into log files via an HTTP request in conjunction with a crafted DNS response, as demonstrated by injecting XSS sequences, related to an "Inverse Lookup Log Corruption (ILLC)" issue	This vulnerability was identified because (1) the version of Microsoft IIS, 6.0, is less than or equal to 6.0.*. Paths: /	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.iis.net/	CVE-2003-1582
148.*.***.*3**	Microsoft IIS: Crafted DNS Response Inverse Lookup Log Corruption XSS	80	**Bajo**	Microsoft Internet Information Services (IIS) 6.0, when DNS resolution is enabled for client IP addresses, allows remote attackers to inject arbitrary text into log files via an HTTP request in conjunction with a crafted DNS response, as demonstrated by injecting XSS sequences, related to an "Inverse Lookup Log Corruption (ILLC)" issue.	This vulnerability was identified because (1) the version of Microsoft IIS, 6.0, is less than or equal to 6.0.*. Paths: /	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.iis.net/	CVE-2003-1582

148.*.***.*3**	Microsoft IIS: Crafted DNS Response Inverse Lookup Log Corruption XSS	9001	**Bajo**	Microsoft Internet Information Services (IIS) 6.0, when DNS resolution is enabled for client IP addresses, allows remote attackers to inject arbitrary text into log files via an HTTP request in conjunction with a crafted DNS response, as demonstrated by injecting XSS sequences, related to an "Inverse Lookup Log Corruption (ILLC)" issue.	This vulnerability was identified because (1) the version of Microsoft IIS, 6.0, is less than or equal to 6.0.*. Paths: /	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.iis.net/	CVE-2003-1582
148.*.***.**5**	Microsoft IIS: Crafted DNS Response Inverse Lookup Log Corruption XSS	80	**Bajo**	Microsoft Internet Information Services (IIS) 6.0, when DNS resolution is enabled for client IP addresses, allows remote attackers to inject arbitrary text into log files via an HTTP request in conjunction with a crafted DNS response, as demonstrated by injecting XSS sequences, related to an "Inverse Lookup Log Corruption (ILLC)" issue.	This vulnerability was identified because (1) the version of Microsoft IIS, 6.0, is less than or equal to 6.0.*.Paths: /	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.iis.net/	CVE-2003-1582

148.*.***.**9**	Possible sensitive directories	80	**Bajo**	A possible sensitive directory has been found. This directory is not directly linked from the website.This check looks for known sensitive directories like: backup directories, database dumps, administration pages, temporary directories. Each of those directories may help an attacker to learn more about his target.	Affected items /Assets/admin /Includes/asp /Includes/css /includes/js/popcalendar.js /Includes/carrusel/javascript/greybox/ventanas.js /Includes/carrusel/javascript/mootools.js /Includes/carrusel/javascript/C2_V4.js /Includes/js/generales.js	Restrict access to this directory or remove it from the website.		
148.*.***.6**	SSL Certificate Expiry	8443	**Bajo**		The SSL certificate of the remote service expired Dec 25 23:48:15 2007 GMT Here is the list of weak SSL ciphers supported by the remote server : Low Strength Ciphers (< 56-bit key) SSLv3 EXP-EDH-			

					RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40) Mac=SHA1 export EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export TLSv1 EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40) Mac=SHA1 export EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export EXP-RC4-			

					MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export			
148.*.***.**8**	Microsoft IIS: Crafted DNS Response Inverse Lookup Log Corruption XSS	443	**Bajo**	Microsoft Internet Information Services (IIS) 6.0, when DNS resolution is enabled for client IP addresses, allows remote attackers to inject arbitrary text into log files via an HTTP request in conjunction with a crafted DNS response, as demonstrated by injecting XSS sequences, related to an "Inverse Lookup Log Corruption (ILLC)" issue.	This vulnerability was identified because (1) the version of Microsoft IIS, 6.0, is less than or equal to 6.0.*. Paths: /	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.iis.net/	CVE-2003-1582

Host	Puerto / Servicio	Host	Puerto / Servicio	Host	Puerto / Servicio
148.***.***.**1	80/TCP – http	148.***.***.4	80/TCP - http	148.***.***.**5	80/TCP - http
148.***.***.**1	25/TCP – smtp	148.***.***.4	5003/TCP - filemaker	148.***.***.**5	7800/TCP - asr
148.***.***.**2	80/TCP – http	148.***.***.4	50003/TCP - unknown	148.***.***.**5	7801/TCP - http
148.***.***.**3	53/UDP – dns	148.***.***.4	50006/TCP - unknown	148.***.***.**6	25/TCP - smtp
148.***.***.**3	53/TCP – dns	148.***.***.5	264/TCP - fw1-topology	148.***.***.**6	80/TCP - http
148.***.***.**4	264/TCP - fw1-topology	148.***.***.6	21/TCP - ftp	148.***.***.**9	25/TCP - smtp
148.***.***.**7	443/TCP – http	148.***.***.6	135/TCP - emap	148.***.***.**9	80/TCP - http

148.***.***.**8	25/TCP – smtp	148.***.***.6	137/TCP - netbios-ns	148.***.***.*3	80/TCP - http
148.***.***.**8	80/TCP – http	148.***.***.6	139/TCP - netbios-ssn	148.***.***.*3	9001/TCP - http
148.***.***.**8	110/TCP - pop3	148.***.***.6	445/TCP - microsoft-ds	148.***.***.*1	80/TCP - http
148.***.***.**8	443/TCP – http	148.***.***.6	1025/TCP - msrpc	148.***.***.*2	80/TCP - http
148.***.***.**8	587/TCP - smtp	148.***.***.6	1433/TCP - ms-sql-s	148.***.***.*2	22/TCP - ssh
148.***.***.1	21/TCP - tcpwrapped	148.***.***.6	3389/TCP - microsoft-rdp	200.***.***.*1	80/TCP - http
148.***.***.1	23/TCP - telnet	148.***.***.6	8443/TCP - http	200.***.***.*1	3389/TCP - microsoft-rdp
148.***.***.1	80/TCP – http	148.***.***.6	8888/TCP - http	200.***.***.*1	5631/TCP - pcanywheredata
148.***.***.1	1720/TCP - H.323/Q.931	148.***.***.6	10000/TCP - snet-sensor-mgmt	148.***.***.2	80/TCP - http
148.***.***.1	5060/TCP - sip-proxy	148.***.***.6	10566/TCP - unknow		

Análisis interno de Vulnerabilidades

Reporte Ejecutivo. Análisis de Vulnerabilidades

Introducción

Este reporte está enfocado plenamente a la detección de vulnerabilidades por lo que los resultados obtenidos deberán ser utilizados para generar un análisis de impacto que permita visualizar el riesgo real para los activos analizados y la información que manejan.

Objetivo

El análisis de vulnerabilidades se orienta a:

- Identificar y analizar cualquier tipo de vulnerabilidad en los activos analizados.
- Orientar al cliente para la mitigación de estas.
- Ofrecer continuidad en el seguimiento de acciones de mitigación.

Herramientas y Técnicas

Los **consultores de resultados** se basan en metodologías de prueba que han sido revisadas y avaladas por la comunidad de seguridad informática para determinar si la red del **organismo receptor** es susceptible de sufrir un ataque informático. Estas prácticas y técnicas de prueba han sido desarrolladas y refinadas constantemente para representar las principales amenazas a las que se encuentra expuesta una empresa con presencia en Internet en la actualidad.
Los **consultores de resultados** utilizan diversos productos de escaneo que son reconocidos como estándares de la industria, como Outpost24 Líder de tecnología en la evaluación de la vulnerabilidad y manejo de redes. Adicionalmente a los programas de escaneo también se utiliza una variedad de herramientas reconocidas como estándares en la industria tales como, NMAP. Los **consultores de resultados** han desarrollado técnicas, scripts y programas en casa que se combinan con los programas anteriormente enumerados para aumentar el alcance y velocidad de la prueba.
Al realizar las pruebas de penetración **consultores de resultados** asumen el papel de atacantes tomando los principios y actitudes mentales que los atacantes utilizan como pensar “outside of the box”. Los servicios de prueba de penetración de los **consultores de resultados** tienen su base en “Open Source Security Testing Methodology Manual” una metodología aprobada y publicada por ISECOM.

Alcance

Analizar específicamente los activos citados a continuación:

10.**.*.2	10.**.**.*8	10.**.**.19
10.**.*.1	10.**.**.*9	10.**.**.20
10.**.*.3	10.**.**.10	10.**.**.21
10.**.*.4	10.**.**.11	10.**.**.22
10.**.*.5	10.**.**.12	10.**.**.23
10.**.*.6	10.**.**.**1	10.**.**.24
10.**.**.*1	10.**.**.**2	10.**.**.25
10.**.**.*2	10.**.**.13	10.**.**.26
10.**.**.*3	10.**.**.14	10.**.**.27
10.**.**.*4	10.**.**.15	10.**.**.**3
10.**.**.*5	10.**.**.16	10.**.**.28
10.**.**.*6	10.**.**.17	10.**.**.29
10.**.**.*7	10.**.**.18	

Análisis de Vulnerabilidades

Durante el análisis realizado a los 38 activos proporcionado por el departamento de Sistemas del **organismo receptor**, fue posible detectar un número considerable de vulnerabilidades. El análisis arrojó las siguientes vulnerabilidades:

Host	Nombre	Alto impacto	Mediano impacto	Bajo impacto	Total de vulnerabilidades	Puertos
10..*.3**	**********.********.gob.mx	0	7	0	7	13
10..*.4**	********.ad.gob	6	16	1	23	23
10..*.5**	********.ad.gob	5	12	1	18	24
10..*.1**	******1.ad.gob	4	10	1	15	11
10..*.2**		4	10	1	15	20
10..*.6**		1	2	0	3	6
10..**.*3**		1	0	0	1	2
10..**.25**	prod.********.gob.mx	0	3	0	3	4
10..**.26**	svn.********.gob.mx	0	10	0	10	5
10..**.**1**		4	4	1	9	8
10..**.**2**	**********.ad.gob	1	2	0	3	11
10..**.13**	*********1.ad.gob	5	6	1	12	19
10..**.19**	*********2.ad.gob	5	6	1	12	19
10..**.20**	*********.ad.gob	4	5	1	10	31
10..**.21**	**********.ad.gob	4	11	1	16	19
10..**.22**	**********.ad.gob	4	4	1	9	8
10..**.10**	********.ad.gob	4	4	1	9	10
10..**.23**	********.ad.gob	4	4	1	9	9

10..**.11**	**********.ad.gob	5	5	1	11	18
10..**.12**	*********.ad.gob	4	4	1	9	9
10..**.*1**		0	1	1	2	4
10..**.24**	www.********.gob.mx	0	1	1	2	3
10..**.*2**		0	1	1	2	3
10..**.*8**		0	1	1	2	3
10..**.*9**		0	1	1	2	2
10..**.15**		0	0	0	0	1
10..**.*4**		0	0	0	0	0
10..**.*5**		0	0	0	0	0
10..**.*6**		0	0	0	0	0
10..**.*7**		0	0	0	0	0
10..**.14**		0	0	0	0	0
10..**.16**		0	0	0	0	0
10..**.17**		0	0	0	0	0
10..**.18**		0	0	0	0	0
10..**.27**		0	0	0	0	0
10..**.**3**		0	0	0	0	0
10..**.28**		0	0	0	0	0
10..**.29**		0	0	0	0	0

Las vulnerabilidades marcadas como **impacto alto** son aquellas que pueden causar mayor impacto al ser explotadas, pudiéndose llevar a cabo actividades riesgosas que pongan en peligro la integridad, confidencialidad o disponibilidad del activo en el que se ejecute dicha vulnerabilidad. Por ejemplo, actividades como: denegación de servicio, acceso no autorizado, publicación de información confidencial, suplantación de identidad, etc.
Las vulnerabilidades marcadas como **impacto medio** son aquellas que pueden no representar un riesgo alto aun que estas puedan afectar la integridad, confidencialidad o disponibilidad de los activos.
Las vulnerabilidades marcadas como **impacto bajo** son aquellas que no causan un alto impacto en los servicios de los activos.

Top de Vulnerabilidades

Los activos categorizados como críticos por el **organismo receptor** cuentan actualmente con las siguientes vulnerabilidades, las cuales se presentan en mayor cantidad.

Vulnerabilidad	Activo	Riesgo	Mitigación
Sesiones Nulas	10.**.**.**1 10.**.**.**2 10.**.**.10 10.**.**.11 10.**.**.12 10.**.**.13 10.**.**.19 10.**.**.20 10.**.**.21	Las sesiones nulas permiten conexiones sin autenticación para enumerar información de la computadora, permitiendo a los atacantes sustraer información valiosa. Al tener conocimiento de los usuarios y sus privilegios, es mucho más fácil conducir un ataque de fuerza bruta contra	Deshabilitar la enumeración de usuarios para así evitar las sesiones nulas. Evitar el uso de cuentas SAM generando una política de

	10.**.**.22 10.**.**.23 10.**.*.2 10.**.*.4 10.**.*.5 10.**.*.1 10.**.**.29	aquellos que son administradores	dominio.
Múltiples vulnerabilidades en parches de actualización de Windows	10.**.**.**1 10.**.**.10 10.**.**.11 10.**.**.12 10.**.**.13 10.**.**.19 10.**.**.20 10.**.**.21 10.**.**.22 10.**.**.23 10.**.*.2 10.**.*.4 10.**.*.5 10.**.*.1 10.**.*.6	Windows contiene múltiples vulnerabilidades desatacando Overflows, permitiendo la ejecución de código remoto arbitrario en todos los activos que presentan versiones obsoletas de Windows .Ataques de negación de Servicios DoS.	Actualizar Windows a la última versión estable
Métodos HTTP soportados DELETE, GET, PUT, TRACE	DELETE,GET,PUT 10.**.*.4 10.**.*.5 TRACE 10.**.**.25 10.**.**.26 10.**.*.3 10.**.*.1	Un atacante puede usar estos métodos para modificar, borrar y tomar control de activo	Deshabilitar estos métodos.
Múltiples vulnerabilidades en la versión de Microsoft IIS	10.**.**.*1 10.**.**.*2 10.**.**.*8 10.**.**.*9 10.**.**.**2 10.**.**.10 10.**.**.11 10.**.**.21 10.**.**.23 10.**.**.24 10.**.*.2 10.**.*.4 10.**.*.5 10.**.*.1 10.**.*.6	Un atacante podría aprovechar este problema para realizar ataques Man-in-the-middle, creación de archivos vía remota	Actualizar a la última versión estable
Múltiples vulnerabilidades en la versión de PHP 5.2.6	10.**.**.26	PHP contiene múltiples vulnerabilidades desatacando Overflows, permitiendo la ejecución de código remoto	Actualizar PHP a la última versión estable

		arbitrario en todos los activos que presentan versiones obsoletas de PHP. Vulnerabilidades en las extensiones SQL permitiendo a atacantes remotos en modo seguro hacer operación LOCALES. Manipulación de cookies.	
Autenticación en texto claro FTP y FTP Anonymous	10.**.**.11 10.**.*.6	Podría permitir a un atacante captar la información de usuario y password, ganando accesos al equipo y tomar el control del activo	Migrar a SSH y/o filtrar accesos. Así como deshabilitar usuario anónimo
Autenticación en texto claro Telnet	10.**.*.3	Podría permitir a un atacante captar la información de usuario y password, ganando accesos al equipo y tomar el control del activo	Migrar a SSH y/o filtrar accesos
DNS recursive queries	10.**.**.13 10.**.**.19 10.**.**.21 10.**.*.4	Cualquier persona puede solicitar una búsqueda de cualquier nombre de dominio. Un atacante puede aprovechar este problema para realizar ataques de envenenamiento de caché contra este servidor de nombres. Si el DNS permite consultas recursivas a través de UDP, esta máquina puede, potencialmente, ser utilizada para 'rebotar' ataques de denegación de servicio contra otras redes o sistemas.	Restringir las consultas recursivas a los anfitriones que debe utilizar este servidor de nombres, como los de la LAN conectados a él.
Múltiples vulnerabilidades en la versión SSL/TLS	10.**.**.**2 10.**.**.21 10.**.**.26 10.**.*.2 10.**.*.3 10.**.*.4 10.**.*.5 10.**.*.1	Las versiones obsoletas y/o el cifrado débil podrían permitir a un atacante escuchar disimuladamente sobre la comunicación que viaja en la red.	Establecer contraseñas robustas en la autenticación y endurecer el tipo de cifrado así como actualizar la versión de SSL a la versión 3
Múltiples vulnerabilidades en OpenSSH	10.**.**.25 10.**.**.26 10.**.*.3 10.**.*.6	Enumeración de las cuentas de autenticación Buffer Management Multiple Overflows	Actualizar a la última versión estable
Múltiples vulnerabilidades en la versión de Apache Tomcat	10.**.*.3	Apache contiene múltiples vulnerabilidades desatacando Overflows, permitiendo la ejecución de código remoto arbitrario, negación de servicios,	Actualizar Apache a la última versión estable

		Cross site scripting en todos los activos que presentan versiones obsoletas de Apache.	

Servicios vulnerables

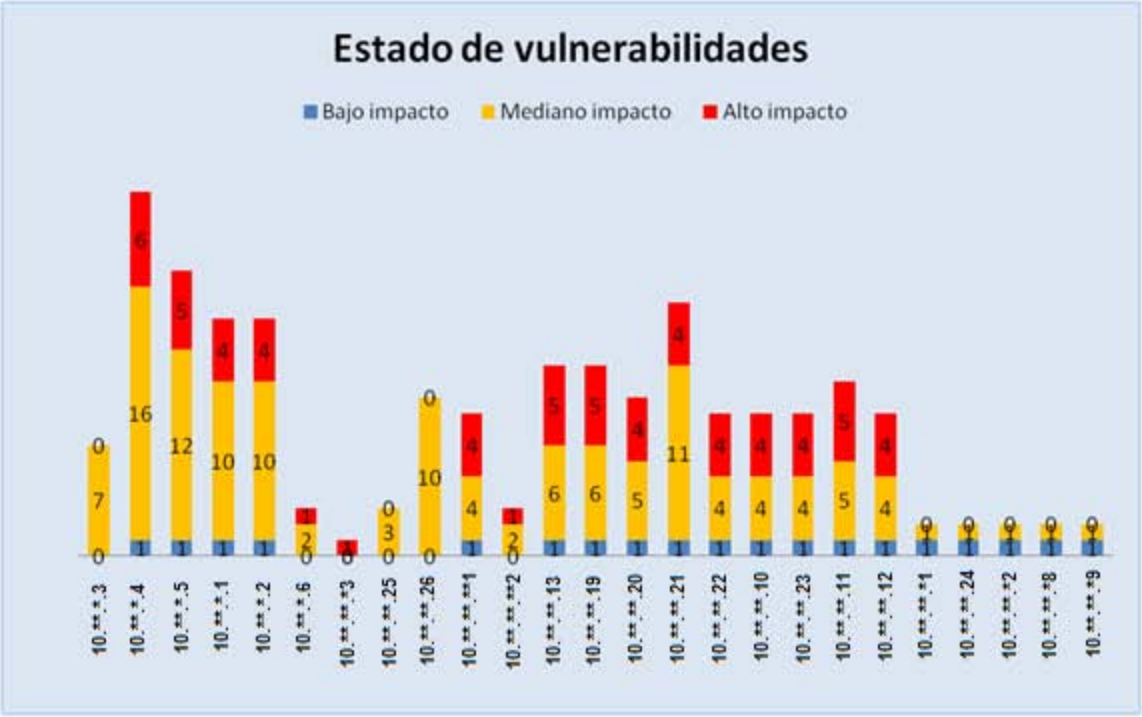
Los activos analizados cuentan actualmente con servicios vulnerables.

Servicio	Puerto	Descripción
SSL / TLS	80 443 3389 8443 8098 5307 3269 636 1311	Puede ser vulnerable si es que dicho servicio contase con una versión obsoleta de los certificados del servicio, ya que proporcionaría accesos débiles para la autenticación.
TELNET	23	Podría ser aprovechado para que un atacante capturara usuario y password ya que viaja en texto claro.
SSH	22	Podría ser aprovechado para que un atacante ejecutara ataques de denegación de servicio e incluso, según el advisory original, ejecutar código arbitrario
HTTP	80	Puede ser un servicio vulnerable porque mediante ese servicio son mandados mensajes que contienen información crítica del sistema, podría permitir a un usuario malintencionado provocar negación de servicios y/o ejecutar código arbitrario en forma remota
DNS	53	Cualquier persona puede solicitar una búsqueda de cualquier nombre de dominio. Un atacante puede aprovechar este problema para realizar ataques de envenenamiento de caché contra este servidor de nombres.
FTP	21	Podría ser aprovechado para que un atacante capturara usuario y password ya que viaja en texto claro.
NetBIOS	137 139	Puede ser un servicio vulnerable porque mediante ese servicio son mandados mensajes que contienen información crítica del sistema. Además netBIOS puede también ser una ventana de intrusión al sistema.
SMB	445	Puede ser vulnerable ya que mediante estos servicios es como Null session se hace posible. Permite accesos anónimos desde cuentas externas. Acepta conexiones anónimas sesiones en forma de Nulas

Estado de vulnerabilidades

En la siguiente gráfica se muestran los índices de vulnerabilidades de acuerdo al nivel de impacto para cada uno de los activos.

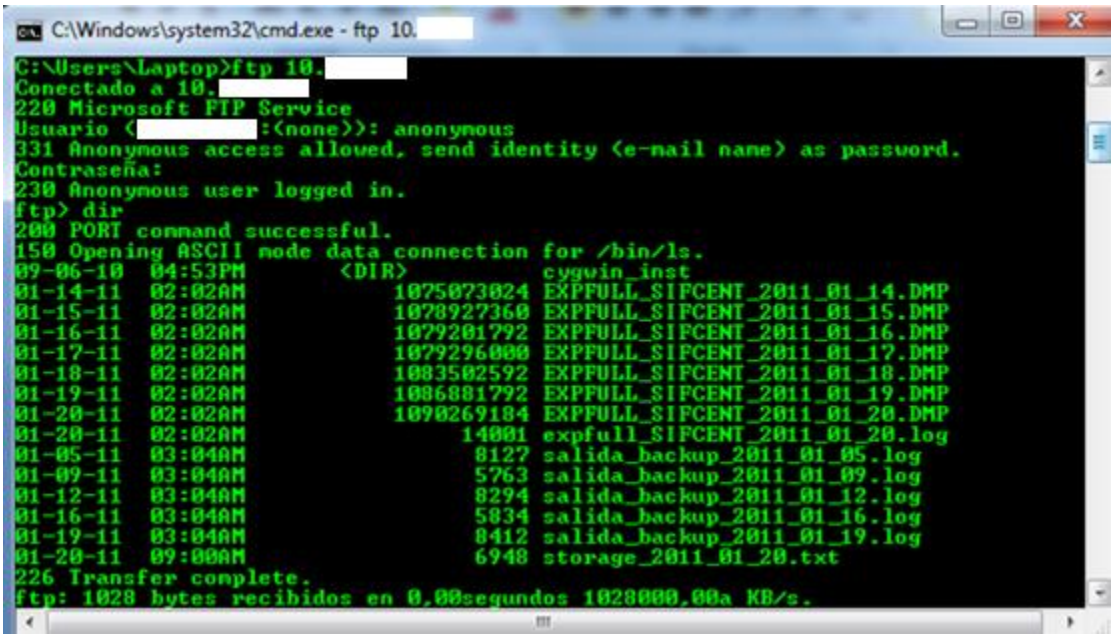
Índice de vulnerabilidades por activo



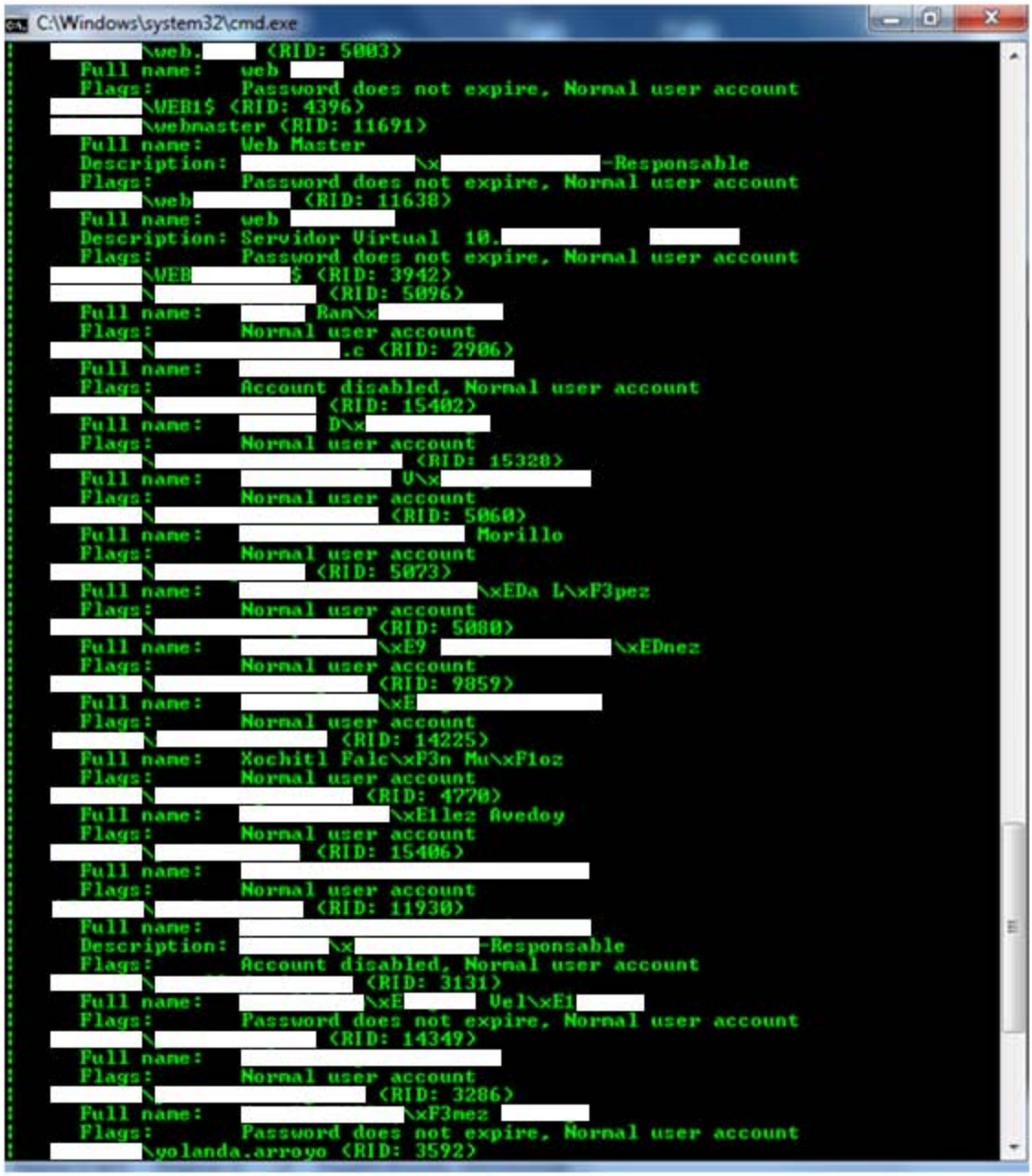
Evidencia de vulnerabilidades

Mediante las comprobaciones manuales realizadas a los activos, se pudo detectar ciertas vulnerabilidades. Por mencionar algunas.

FTP Anónimo



Enumeración de usuarios.



Anexos

Detalle técnico de cada uno de los activos.

Host	Vulnerabilidad	Puerto	Factor de Impacto	Descripción	Información	Solución	Referencia	CVE
10..**.29**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474 url - http://support.microsoft.com/?kbid=823659 url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	
10..**.11**	FTP Anonymous Login Detection	21	Alto	The remote host is running an FTP server. This FTP server allows anonymous logins. If it is not desirable for everyone to log in to the FTP server then you should deactivate the anonymous account.				CVE-1999-0497

10..**.**1**	Microsoft Windows: Graphics Rendering Engine Could Allow Remote Code Execution	445	Alto	Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Microsoft Graphics Rendering Engine in Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unsplecified Office document containing a thumbnail bitmap with a negative biClrUsed value, as reported by Moti and Xu Hao.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows solution - http://www.microsoft.com/technet/security/advisory/2490606.mspx	CVE-2010-3970
10..**.**1**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474 url - http://support.microsoft.com/?kbid=823659 url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	

10..**.**1**	Microsoft Windows: win32k.sys CreateDIBPalette() Function Local Overflow	445	Alto	Buffer overflow in the CreateDIBPalette function in win32k.sys allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged the existence of this vulnerability, but not yet provided a solution. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-2739
10..**.**1**	Microsoft Windows: win32k.sys Driver GreEnableEUDC() Function Overflow	445	Alto	Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG_BINARY value for a SystemDefaultEUDCFont registry key.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged this issue and is currently working on a solution.	url - http://microsoft.com/windows	CVE-2010-4398

10..**.**2**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474url - http://support.microsoft.com/?kbid=823659url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	
10..**.10**	Microsoft Windows: Graphics Rendering Engine Could Allow Remote Code Execution	445	Alto	Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Microsoft Graphics Rendering Engine in Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unsplecified Office document containing a thumbnail bitmap with a negative biClrUsed value, as reported by Moti and Xu Hao.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows solution - http://www.microsoft.com/technet/security/advisory/2490606.mspx	CVE-2010-3970

10..**.10**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474 url - http://support.microsoft.com/?kbid=823659 url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	
10..**.10**	Microsoft Windows: win32k.sys CreateDIBPalette() Function Local Overflow	445	Alto	Buffer overflow in the CreateDIBPalette function in win32k.sys allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged the existence of this vulnerability, but not yet provided a solution. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-2739

10..**.10**	Microsoft Windows: win32k.sys Driver GreEnableEUDC() Function Overflow	445	Alto	Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG_BINARY value for a SystemDefaultEUDCFont registry key.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged this issue and is currently working on a solution.	url - http://microsoft.com/windows	CVE-2010-4398
10..**.11**	Microsoft Windows: Graphics Rendering Engine Could Allow Remote Code Execution	445	Alto	Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Microsoft Graphics Rendering Engine in Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unsplecified Office document containing a thumbnail bitmap with a negative biClrUsed value, as reported by Moti and Xu Hao.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows solution - http://www.microsoft.com/technet/security/advisory/2490606.mspx	CVE-2010-3970

10..**.11**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474url - http://support.microsoft.com/?kbid=823659url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	
10..**.11**	Microsoft Windows: win32k.sys CreateDIBPalette() Function Local Overflow	445	Alto	Buffer overflow in the CreateDIBPalette function in win32k.sys allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged the existence of this vulnerability, but not yet provided a solution. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-2739

10..**.11**	Microsoft Windows: win32k.sys Driver GreEnableEUDC() Function Overflow	445	Alto	Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG_BINARY value for a SystemDefaultEUDCFont registry key.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged this issue and is currently working on a solution.	url - http://microsoft.com/windows	CVE-2010-4398
10..**.12**	Microsoft Windows: Graphics Rendering Engine Could Allow Remote Code Execution	445	Alto	Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Microsoft Graphics Rendering Engine in Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unsplecified Office document containing a thumbnail bitmap with a negative biClrUsed value, as reported by Moti and Xu Hao.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows solution - http://www.microsoft.com/technet/security/advisory/2490606.mspx	CVE-2010-3970

10..**.12**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474 url - http://support.microsoft.com/?kbid=823659 url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	
10..**.12**	Microsoft Windows: win32k.sys CreateDIBPalette() Function Local Overflow	445	Alto	Buffer overflow in the CreateDIBPalette function in win32k.sys allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged the existence of this vulnerability, but not yet provided a solution. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-2739

10..**.12**	Microsoft Windows: win32k.sys Driver GreEnableEUDC() Function Overflow	445	Alto	Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG_BINARY value for a SystemDefaultEUDCFont registry key.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged this issue and is currently working on a solution.	url - http://microsoft.com/windows	CVE-2010-4398
10..**.13**	Microsoft Windows: Graphics Rendering Engine Could Allow Remote Code Execution	445	Alto	Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Microsoft Graphics Rendering Engine in Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unsplecified Office document containing a thumbnail bitmap with a negative biClrUsed value, as reported by Moti and Xu Hao.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows solution - http://www.microsoft.com/technet/security/advisory/2490606.mspx	CVE-2010-3970
10..**.13**	Anonymous SMB Login Enabled	445	Alto	Anonymous access to this SMB service is enabled. If this is an internet-facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	solution - http://support.microsoft.com/?kbid=246261	

10..**.13**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474 url - http://support.microsoft.com/?kbid=823659 url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	
10..**.13**	Microsoft Windows: win32k.sys CreateDIBPalette() Function Local Overflow	445	Alto	Buffer overflow in the CreateDIBPalette function in win32k.sys allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged the existence of this vulnerability, but not yet provided a solution. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-2739

10..**.13**	Microsoft Windows: win32k.sys Driver GreEnableEUDC() Function Overflow	445	Alto	Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG_BINARY value for a SystemDefaultEUDCFont registry key.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged this issue and is currently working on a solution.	url - http://microsoft.com/windows	CVE-2010-4398
10..**.19**	Microsoft Windows: Graphics Rendering Engine Could Allow Remote Code Execution	445	Alto	Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Microsoft Graphics Rendering Engine in Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unsplecified Office document containing a thumbnail bitmap with a negative biClrUsed value, as reported by Moti and Xu Hao.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows solution - http://www.microsoft.com/technet/security/advisory/2490606.mspx	CVE-2010-3970
10..**.19**	Anonymous SMB Login Enabled	445	Alto	Anonymous access to this SMB service is enabled. If this is an internet-facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	solution - http://support.microsoft.com/?kbid=246261	

10..**.19**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474url - http://support.microsoft.com/?kbid=823659url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	
10..**.19**	Microsoft Windows: win32k.sys CreateDIBPalette() Function Local Overflow	445	Alto	Buffer overflow in the CreateDIBPalette function in win32k.sys allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged the existence of this vulnerability, but not yet provided a solution. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-2739

10..**.19**	Microsoft Windows: win32k.sys Driver GreEnableEUDC() Function Overflow	445	Alto	Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG_BINARY value for a SystemDefaultEUDCFont registry key.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged this issue and is currently working on a solution.	url - http://microsoft.com/windows	CVE-2010-4398
10..**.20**	Microsoft Windows: Graphics Rendering Engine Could Allow Remote Code Execution	445	Alto	Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Microsoft Graphics Rendering Engine in Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unsplecified Office document containing a thumbnail bitmap with a negative biClrUsed value, as reported by Moti and Xu Hao.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows solution - http://www.microsoft.com/technet/security/advisory/2490606.mspx	CVE-2010-3970

10..**.20**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474 url - http://support.microsoft.com/?kbid=823659 url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	
10..**.20**	Microsoft Windows: win32k.sys CreateDIBPalette() Function Local Overflow	445	Alto	Buffer overflow in the CreateDIBPalette function in win32k.sys allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged the existence of this vulnerability, but not yet provided a solution. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-2739

10..**.20**	Microsoft Windows: win32k.sys Driver GreEnableEUDC() Function Overflow	445	Alto	Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG_BINARY value for a SystemDefaultEUDCFont registry key.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged this issue and is currently working on a solution.	url - http://microsoft.com/windows	CVE-2010-4398
10..**.21**	Microsoft Windows: Graphics Rendering Engine Could Allow Remote Code Execution	445	Alto	Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Microsoft Graphics Rendering Engine in Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unsplecified Office document containing a thumbnail bitmap with a negative biClrUsed value, as reported by Moti and Xu Hao.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows solution - http://www.microsoft.com/technet/security/advisory/2490606.mspx	CVE-2010-3970

10..**.21**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474 url - http://support.microsoft.com/?kbid=823659 url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	
10..**.21**	Microsoft Windows: win32k.sys CreateDIBPalette() Function Local Overflow	445	Alto	Buffer overflow in the CreateDIBPalette function in win32k.sys allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged the existence of this vulnerability, but not yet provided a solution. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-2739

10..**.21**	Microsoft Windows: win32k.sys Driver GreEnableEUDC() Function Overflow	445	Alto	Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG_BINARY value for a SystemDefaultEUDCFont registry key.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged this issue and is currently working on a solution.	url - http://microsoft.com/windows	CVE-2010-4398
10..**.22**	Microsoft Windows: Graphics Rendering Engine Could Allow Remote Code Execution	445	Alto	Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Microsoft Graphics Rendering Engine in Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unsplecified Office document containing a thumbnail bitmap with a negative biClrUsed value, as reported by Moti and Xu Hao.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows solution - http://www.microsoft.com/technet/security/advisory/2490606.mspx	CVE-2010-3970

10..**.22**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474 url - http://support.microsoft.com/?kbid=823659 url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	
10..**.22**	Microsoft Windows: win32k.sys CreateDIBPalette() Function Local Overflow	445	Alto	Buffer overflow in the CreateDIBPalette function in win32k.sys allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged the existence of this vulnerability, but not yet provided a solution. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-2739

10..**.22**	Microsoft Windows: win32k.sys Driver GreEnableEUDC() Function Overflow	445	Alto	Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG_BINARY value for a SystemDefaultEUDCFont registry key.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged this issue and is currently working on a solution.	url - http://microsoft.com/windows	CVE-2010-4398
10..**.23**	Microsoft Windows: Graphics Rendering Engine Could Allow Remote Code Execution	445	Alto	Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Microsoft Graphics Rendering Engine in Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unsplecified Office document containing a thumbnail bitmap with a negative biClrUsed value, as reported by Moti and Xu Hao.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows solution - http://www.microsoft.com/technet/security/advisory/2490606.mspx	CVE-2010-3970

10..**.23**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474 url - http://support.microsoft.com/?kbid=823659 url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	
10..**.23**	Microsoft Windows: win32k.sys CreateDIBPalette() Function Local Overflow	445	Alto	Buffer overflow in the CreateDIBPalette function in win32k.sys allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged the existence of this vulnerability, but not yet provided a solution. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-2739

10..**.23**	Microsoft Windows: win32k.sys Driver GreEnableEUDC() Function Overflow	445	Alto	Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG_BINARY value for a SystemDefaultEUDCFont registry key.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged this issue and is currently working on a solution.	url - http://microsoft.com/windows	CVE-2010-4398
10..*.2**	Microsoft Windows: Graphics Rendering Engine Could Allow Remote Code Execution	445	Alto	Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Microsoft Graphics Rendering Engine in Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unsplecified Office document containing a thumbnail bitmap with a negative biClrUsed value, as reported by Moti and Xu Hao.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows solution - http://www.microsoft.com/technet/security/advisory/2490606.mspx	CVE-2010-3970

10..*.2**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474url - http://support.microsoft.com/?kbid=823659url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	
10..*.2**	Microsoft Windows: win32k.sys CreateDIBPalette() Function Local Overflow	445	Alto	Buffer overflow in the CreateDIBPalette function in win32k.sys allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged the existence of this vulnerability, but not yet provided a solution. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-2739

10..*.2**	Microsoft Windows: win32k.sys Driver GreEnableEUDC() Function Overflow	445	Alto	Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG_BINARY value for a SystemDefaultEUDCFont registry key.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged this issue and is currently working on a solution.	url - http://microsoft.com/windows	CVE-2010-4398
10..*.4**	Microsoft Windows: Graphics Rendering Engine Could Allow Remote Code Execution	445	Alto	Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Microsoft Graphics Rendering Engine in Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unsplecified Office document containing a thumbnail bitmap with a negative biClrUsed value, as reported by Moti and Xu Hao.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows solution - http://www.microsoft.com/technet/security/advisory/2490606.mspx	CVE-2010-3970
10..*.4**	Anonymous SMB Login Enabled	445	Alto	Anonymous access to this SMB service is enabled. If this is an internet-facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	solution - http://support.microsoft.com/?kbid=246261	

10..*.4**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474 url - http://support.microsoft.com/?kbid=823659 url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	
10..*.4**	Microsoft Windows: win32k.sys CreateDIBPalette() Function Local Overflow	445	Alto	Buffer overflow in the CreateDIBPalette function in win32k.sys allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged the existence of this vulnerability, but not yet provided a solution. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-2739

10..*.4**	Microsoft Windows: win32k.sys Driver GreEnableEUDC() Function Overflow	445	Alto	Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG_BINARY value for a SystemDefaultEUDCFont registry key.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged this issue and is currently working on a solution.	url - http://microsoft.com/windows	CVE-2010-4398
10..*.4**	HTTP Options Supported	80	Alto	The following options are supported by the web server running on this port.	OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH			
10..*.5**	Microsoft Windows: Graphics Rendering Engine Could Allow Remote Code Execution	445	Alto	Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Microsoft Graphics Rendering Engine in Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unsplecified Office document containing a thumbnail bitmap with a	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows solution - http://www.microsoft.com/technet/security/advisory/2490606.mspx	CVE-2010-3970

				negative biClrUsed value, as reported by Moti and Xu Hao.				
10..*.5**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474 url - http://support.microsoft.com/?kbid=823659 url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	

10..*.5**	Microsoft Windows: win32k.sys CreateDIBPalette() Function Local Overflow	445	Alto	Buffer overflow in the CreateDIBPalette function in win32k.sys allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged the existence of this vulnerability, but not yet provided a solution. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-2739
10..*.5**	Microsoft Windows: win32k.sys Driver GreEnableEUDC() Function Overflow	445	Alto	Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG_BINARY value for a SystemDefaultEUDCFont registry key.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged this issue and is currently working on a solution.	url - http://microsoft.com/windows	CVE-2010-4398
10..*.5**	HTTP Options Supported	443	Alto	The following options are supported by the web server running on this port.	OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND,			

					PROPPATCH, LOCK, UNLOCK, SEARCH			
10..*.1**	Microsoft Windows: Graphics Rendering Engine Could Allow Remote Code Execution	445	Alto	Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Microsoft Graphics Rendering Engine in Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unsplecified Office document containing a thumbnail bitmap with a negative biClrUsed value, as reported by Moti and Xu Hao.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows solution - http://www.microsoft.com/technet/security/advisory/2490606.mspx	CVE-2010-3970

10..*.1**	SMB Null Sessions Enabled	445	Alto	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet facing server, having anonymous access to it is generally a bad idea.		Reconfigure this service.	url - http://support.microsoft.com/?kbid=143474url - http://support.microsoft.com/?kbid=823659url - http://technet.microsoft.com/en-us/library/dd349805.aspx#BKMK_44	
10..*.1**	Microsoft Windows: win32k.sys CreateDIBPalette() Function Local Overflow	445	Alto	Buffer overflow in the CreateDIBPalette function in win32k.sys allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged the existence of this vulnerability, but not yet provided a solution. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-2739

10..*.1**	Microsoft Windows: win32k.sys Driver GreEnableEUDC() Function Overflow	445	Alto	Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG_BINARY value for a SystemDefaultEUDCFont registry key.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has acknowledged this issue and is currently working on a solution.	url - http://microsoft.com/windows	CVE-2010-4398
10..*.6**	FTP Anonymous Login Detection	21	Alto	The remote host is running an FTP server. This FTP server allows anonymous logins. If it is not desirable for everyone to log in to the FTP server then you should deactivate the anonymous account.				CVE-1999-0497

10..**.**1**	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability	445	**Medio**	Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.microsoft.com/	CVE-2007-1912
10..**.**1**	Microsoft Windows: PostMessage function with 0x4c value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x4c value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1735

10..**.**1**	Microsoft Windows: PostMessage function with 0x18d value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x18d value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1734
10..**.**1**	Microsoft Windows: Unspecified API Argument Validation Local DoS	445	**Medio**	An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-0719

10..**.**2**	SSL/TLS Renegotiation Handshakes Man-in-the-Middle Plaintext Data Injection	3389	**Medio**	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS), mod_ssl in the Apache HTTP Server, OpenSSL, Mozilla Network Security Services (NSS), multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context.		OpenSSL has provided a fix for this in version 0.9.8m and later. Microsoft has released a workaround to disable renegotiation.	solution - http://www.openssl.org/source/ solution - http://support.microsoft.com/kb/977377 solution - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555	CVE-2009-3555

10..**.**2**	SSL/TLS Cipher Suite Detect MD5	3389	**Medio**	The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5 in the signature algorithm of an X.509 certificate.	---------- [TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium]	Reconfigure the service to disallow the listed cipher suites	url - http://www.kb.cert.org/vuls/id/836068	CVE-2004-2761
10..**.10**	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability	445	**Medio**	Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.microsoft.com/	CVE-2007-1912

10..**.10**	Microsoft Windows: PostMessage function with 0x4c value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x4c value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1735
10..**.10**	Microsoft Windows: PostMessage function with 0x18d value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x18d value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1734

10..**.10**	Microsoft Windows: Unspecified API Argument Validation Local DoS	445	**Medio**	An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-0719
10..**.11**	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability	445	**Medio**	Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.microsoft.com/	CVE-2007-1912

10..**.11**	Microsoft Windows: PostMessage function with 0x4c value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x4c value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1735
10..**.11**	Microsoft Windows: PostMessage function with 0x18d value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x18d value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1734

10..**.11**	Microsoft Windows: Unspecified API Argument Validation Local DoS	445	**Medio**	An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-0719
10..**.11**	Microsoft FTP Service LIST -R Stack Consumption Denial of Service Vulnerability	21	**Medio**	Stack consumption vulnerability in the FTP server in Microsoft Internet Information Server (IIS) 5.0 and 6.0 allows remote authenticated users to cause a denial of service (crash) via a list (ls) -R command containing a wildcard that references a subdirectory, followed by a .. (dot dot).	This vulnerability was identified because (1) the version of Microsoft FTP Server, 6.0, is less than or equal to 7.5. Paths: /	Upgrade to the latest version of Microsoft IIS.	solution - http://www.microsoft.com/technet/security/Bulletin/MS09-053.mspx solution - http://www.microsoft.com/technet/security/advisory/975191.mspx	CVE-2009-2521

10..**.12**	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability	445	**Medio**	Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.microsoft.com/	CVE-2007-1912
10..**.12**	Microsoft Windows: PostMessage function with 0x4c value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x4c value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1735

10..**.12**	Microsoft Windows: PostMessage function with 0x18d value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x18d value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1734
10..**.12**	Microsoft Windows: Unspecified API Argument Validation Local DoS	445	**Medio**	An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-0719

10..**.13**	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability	445	**Medio**	Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.microsoft.com/	CVE-2007-1912

10..**.13**	DNS recursive queries	53	**Medio**	This DNS appears to allow recursive queries (i.e. requests for lookupsof third party names).In other words, anyone may request a lookup of any domain name. An attacker can take advantage of this problem to perform cache poisoning attacks againstthis nameserver.If the DNS allows recursive queries over UDP, this host can potentially alsobe used to 'bounce' denial of service attacks against other networks or systems.Note: If this nameserver is your internal nameserver, and the scan was performedfrom within your network, you may disregard this notice.		Restrict recursive queries to the hosts that should use this nameserver, such as those of the LAN connected to it.If you are using a Microsoft DNS sever, follow the applicable instructionsat the following URL: http://www.eukhost.com/forums/archive/index.php/t-852.htmlIf you are using bind 8, this can be done by using the instruction'allow-recursion' in the 'options' section of your 'named.conf'.If you are using bind 9, you can define a grouping of internal addressesusing the 'acl' command.Then, within the	url - http://www.subneural.net/files/bind9arm.pdfurl - http://technet2.microsoft.com/WindowsServer/en/library/e1fe9dff-e87b-44ae-ac82-8e76d19d9c371033.mspx	

						options block, you can explicitly state: allow-recursion {hosts_defined_in_acl}'If you are using another name server, consult its documentation.		

10..**.13**	DNS recursive queries	53	**Medio**	This DNS appears to allow recursive queries (i.e. requests for lookups of third party names). In other words, anyone may request a lookup of any domain name. An attacker can take advantage of this problem to perform cache poisoning attacks against this nameserver. If the DNS allows recursive queries over UDP, this host can potentially also be used to 'bounce' denial of service attacks against other networks or systems. Note: If this nameserver is your internal nameserver, and the scan was performed from within your network, you may disregard this notice.		Restrict recursive queries to the hosts that should use this nameserver, such as those of the LAN connected to it. If you are using a Microsoft DNS sever, follow the applicable instructions at the following URL: http://www.eukhost.com/forums/archive/index.php/t-852.html If you are using bind 8, this can be done by using the instruction 'allow-recursion' in the 'options' section of your 'named.conf'. If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command.	url - http://www.subneural.net/files/bind9arm.pdf url - http://technet2.microsoft.com/WindowsServer/en/library/e1fe9dff-e87b-44ae-ac82-8e76d19d9c371033.mspx	

						Then, within the options block, you can explicitly state: allow-recursion {hosts_defined_in_acl}' If you are using another name server, consult its documentation.		

10..**.13**	Microsoft Windows: PostMessage function with 0x4c value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x4c value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1735
10..**.13**	Microsoft Windows: PostMessage function with 0x18d value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x18d value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1734

10..**.13**	Microsoft Windows: Unspecified API Argument Validation Local DoS	445	**Medio**	An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-0719
10..**.19**	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability	445	**Medio**	Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.microsoft.com/	CVE-2007-1912

10..**.19**	DNS recursive queries	53	**Medio**	This DNS appears to allow recursive queries (i.e. requests for lookups of third party names). In other words, anyone may request a lookup of any domain name. An attacker can take advantage of this problem to perform cache poisoning attacks against this nameserver. If the DNS allows recursive queries over UDP, this host can potentially also be used to 'bounce' denial of service attacks against other networks or systems. Note: If this nameserver is your internal nameserver, and the scan was performed from within your network, you may disregard this notice.		Restrict recursive queries to the hosts that should use this nameserver, such as those of the LAN connected to it. If you are using a Microsoft DNS sever, follow the applicable instructions at the following URL: http://www.eukhost.com/forums/archive/index.php/t-852.html If you are using bind 8, this can be done by using the instruction 'allow-recursion' in the 'options' section of your 'named.conf'. If you are using bind 9, you can define a grouping of internal addresses	url - http://www.subneural.net/files/bind9arm.pdf url - http://technet2.microsoft.com/WindowsServer/en/library/e1fe9dff-e87b-44ae-ac82-8e76d19d9c371033.mspx	

						using the 'acl' command. Then, within the options block, you can explicitly state: allow-recursion {hosts_defined_in_acl}' If you are using another name server, consult its documentation.		

10..**.19**	DNS recursive queries	53	**Medio**	This DNS appears to allow recursive queries (i.e. requests for lookupsof third party names).In other words, anyone may request a lookup of any domain name. An attacker can take advantage of this problem to perform cache-poisoning attacks againstthis nameserver.If the DNS allows recursive queries over UDP, this host can potentially alsobe used to 'bounce' denial of service attacks against other networks or systems.Note: If this nameserver is your internal nameserver, and the scan was performedfrom within your network, you may disregard this notice.		Restrict recursive queries to the hosts that should use this nameserver, such as those of the LAN connected to it.If you are using a Microsoft DNS sever, follow the applicable instructionsat the following URL: http://www.eukhost.com/forums/archive/index.php/t-852.htmlIf you are using bind 8, this can be done by using the instruction'allow-recursion' in the 'options' section of your 'named.conf'.If you are using bind 9, you can define a grouping of internal addressesusing the 'acl' command.Then, within the	url - http://www.subneural.net/files/bind9arm.pdfurl - http://technet2.microsoft.com/WindowsServer/en/library/e1fe9dff-e87b-44ae-ac82-8e76d19d9c371033.mspx	

						options block, you can explicitly state: allow-recursion {hosts_defined_in_acl}'If you are using another name server, consult its documentation.		

10..**.19**	Microsoft Windows: PostMessage function with 0x4c value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x4c value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1735
10..**.19**	Microsoft Windows: PostMessage function with 0x18d value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x18d value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1734

10..**.19**	Microsoft Windows: Unspecified API Argument Validation Local DoS	445	**Medio**	An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-0719
10..**.20**	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability	445	**Medio**	Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.microsoft.com/	CVE-2007-1912

10..**.20**	Microsoft Windows: PostMessage function with 0x4c value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x4c value as the second argument.Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1735
10..**.20**	Microsoft Windows: PostMessage function with 0x18d value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x18d value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1734

10..**.20**	Microsoft Windows: Unspecified API Argument Validation Local DoS	445	**Medio**	An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-0719

10..**.20**	MySQL MyISAM Table Privileges Secuity Bypass Vulnerability	3306	**Medio**	MySQL 4.1.x before 4.1.24, 5.0.x before 5.0.60, 5.1.x before 5.1.24, and 6.0.x before 6.0.5 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are within the MySQL home data directory, which can point to tables that are created in the future.	This vulnerability was identified because (1) the version of MySQL, 4.1.23-pro-nt, is less than 4.1.24.	Upgrade to version 5.0.92, 5.1.49, 5.5.5 or 6.0.14 or later of MySQL.	url - http://dev.mysql.com/doc/refman/6.0/en/news-6-0-5.html url - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-24.html url - http://dev.mysql.com/doc/refman/5.0/en/releasenotes-es-5-0-60.html url - http://dev.mysql.com/doc/refman/4.1/en/news-4-1-24.html	CVE-2008-2079

10..**.21**	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability	445	**Medio**	Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.microsoft.com/	CVE-2007-1912

10..**.21**	SSL/TLS Renegotiation Handshakes Man-in-the-Middle Plaintext Data Injection	8443	**Medio**	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS), mod_ssl in the Apache HTTP Server, OpenSSL, Mozilla Network Security Services (NSS), multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context.		OpenSSL has provided a fix for this in version 0.9.8m and later.Microsoft has released a workaround to disable renegotiation.	solution - http://www.openssl.org/source/solution - http://support.microsoft.com/kb/977377 solution - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555	CVE-2009-3555

10..**.21**	SSL/TLS Weak and Export Ciphers Detected	8443	**Medio**	The service running on this port allows the use of weak encryption ciphers, which might allow an attacker to eavesdrop on the communication.	---------- [SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_EXPORT_WITH_DES40_CBC_SHA][EXP-DES-CBC-SHA][56][40][export] [RSA_WITH_DES_CBC_SHA][DES-CBC-SHA][56][56][weak] [DHE_RSA_EXPORT_WITH_DES40_CBC_SHA][EXP-EDH-RSA-DES-CBC-SHA][56][40][export	For Apache, add the following line to the configuration file (e.g. httpd.conf): SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM and restart the server. For Microsoft IIS, set the following registry keys to 0: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL	url - http://support.microsoft.com/default.aspx?scid=kb;en-us;245030 url - http://blog.stardothosting.com/2009/05/22/testing-for-weak-ssl-ciphers-for-security-audits/ url - http://www.routerzone.eu/wiki/index.php/Restricting_Weak_SSL_Ciphers,_F5_BigIP url - http://www.openssl.org/docs/apps/ciphers.html solution - http://blog.zenone.org/2009/03/pci-compliance-disable-sslv2-and-weak.html	

					] [DHE_RSA_WITH_DES_CBC_SHA][EDH-RSA-DES-CBC-SHA][56][56][weak] --- [TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] --- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_EXPORT_WITH_DES40_CBC_SHA][EXP-DES-CBC-SHA][56][40][export]	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\C		

					[RSA_WITH_DES_CBC_SHA][DES-CBC-SHA][56][56][weak] [DHE_RSA_EXPORT_WITH_DES40_CBC_SHA][EXP-EDH-RSA-DES-CBC-SHA][56][40][export] [DHE_RSA_WITH_DES_CBC_SHA][EDH-RSA-DES-CBC-SHA][56][56][weak]	iphers\RC4 64/128		

10..**.21**	DNS recursive queries	53	**Medio**	This DNS appears to allow recursive queries (i.e. requests for lookups of third party names). In other words, anyone may request a lookup of any domain name. An attacker can take advantage of this problem to perform cache poisoning attacks against this nameserver. If the DNS allows recursive queries over UDP, this host can potentially also be used to 'bounce' denial of service attacks against other networks or systems. Note: If this nameserver is your internal nameserver, and the scan was performed from within your network, you may disregard this notice.		Restrict recursive queries to the hosts that should use this nameserver, such as those of the LAN connected to it. If you are using a Microsoft DNS sever, follow the applicable instructions at the following URL: http://www.eukhost.com/forums/archive/index.php/t-852.html If you are using bind 8, this can be done by using the instruction 'allow-recursion' in the 'options' section of your 'named.conf'. If you are using bind 9, you can define a grouping of internal addresses using the 'acl'	url - http://www.subneural.net/files/bind9arm.pdf url - http://technet2.microsoft.com/WindowsServer/en/library/e1fe9dff-e87b-44ae-ac82-8e76d19d9c371033.mspx	

						command. Then, within the options block, you can explicitly state: allow-recursion {hosts_defined_in_acl}' If you are using another name server, consult its documentation.		

10..**.21**	DNS recursive queries	53	**Medio**	This DNS appears to allow recursive queries (i.e. requests for lookupsof third party names).In other words, anyone may request a lookup of any domain name. An attacker can take advantage of this problem to perform cache poisoning attacks againstthis nameserver.If the DNS allows recursive queries over UDP, this host can potentially alsobe used to 'bounce' denial of service attacks against other networks or systems.Note: If this nameserver is your internal nameserver, and the scan was performedfrom within your network, you may disregard this notice.		Restrict recursive queries to the hosts that should use this nameserver, such as those of the LAN connected to it.If you are using a Microsoft DNS sever, follow the applicable instructionsat the following URL: http://www.eukhost.com/forums/archive/index.php/t-852.htmlIf you are using bind 8, this can be done by using the instruction'allow-recursion' in the 'options' section of your 'named.conf'.If you are using bind 9, you can define a grouping of internal addressesusing the 'acl' command.Then, within the	url - http://www.subneural.net/files/bind9arm.pdfurl - http://technet2.microsoft.com/WindowsServer/en/library/e1fe9dff-e87b-44ae-ac82-8e76d19d9c371033.mspx	

						options block, you can explicitly state: allow-recursion {hosts_defined_in_acl}'If you are using another name server, consult its documentation.		

10..**.21**	SSL Certificate Authenticity	8443	**Medio**	The certificate presented by this service does not seem to have been issued by a valid Certificate Authority (CA). By having a trusted CA sign your certificate, they certify that you are in fact you. Note: This finding is issued if it is not possible to verify the authenticity of the certificate presented by the service, and is sometimes a result of the service being misconfigured. Any SSLv3/TLSv1 compliant service must present the complete chain of certificates used to sign its own, optionally excluding the root CA certificate. A more detailed reason for why the chain of trust was broken is listed in the table in the information section of this finding.	---------- [depth][country][state][locality][organization][common name][error] ---------- [0][US][CA][Fremont][symantec.com][antivirusviv][self signed certificate]	Use a valid Certificate Authority (CA)		
10..**.21**	SSL/TLS Cipher Suite Detect MD5	8443	**Medio**	The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by	---------- [SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm	Reconfigure the service to disallow the listed cipher suites	url - http://www.kb.cert.org/vuls/id/836068	CVE-2004-2761

				attacks on the use of MD5 in the signature algorithm of an X.509 certificate.	Bits][Bits Used][Cipher Strength] [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium] [TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium]			

10..**.21**	SSL Certificate Name Mismatch	8443	**Medio**	The SSL certificate used by this service is not valid for the domain name where this service is located. This could allow for man-in-the-middle attacks.	None of the subject common names (antivirusviv) match any of the following domains: antivirusviv.ad.gob and 10.**.**.21.	Using certificates with mismatched names is fine for development or testing servers but,for production servers a completely valid certificate should be used. If thishost is a production server, you should purchase and install a server certificatesigned by a trusted Certificate Authority. Ensure that the domain where the certificate is usedmatches the domain encoded in the certificate.	solution - http://www.digicert.com/ssl-support/certificate-name-mismatch-error.htm	

10..**.21**	Microsoft Windows: PostMessage function with 0x4c value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x4c value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1735
10..**.21**	Microsoft Windows: PostMessage function with 0x18d value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x18d value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1734

10..**.21**	Microsoft Windows: Unspecified API Argument Validation Local DoS	445	**Medio**	An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-0719
10..**.22**	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability	445	**Medio**	Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.microsoft.com/	CVE-2007-1912

10..**.22**	Microsoft Windows: PostMessage function with 0x4c value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x4c value as the second argument.Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1735
10..**.22**	Microsoft Windows: PostMessage function with 0x18d value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x18d value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1734

10..**.22**	Microsoft Windows: Unspecified API Argument Validation Local DoS	445	**Medio**	An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-0719
10..**.23**	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability	445	**Medio**	Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.microsoft.com/	CVE-2007-1912

10..**.23**	Microsoft Windows: PostMessage function with 0x4c value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x4c value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1735
10..**.23**	Microsoft Windows: PostMessage function with 0x18d value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x18d value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1734

10..**.23**	Microsoft Windows: Unspecified API Argument Validation Local DoS	445	**Medio**	An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-0719
10..**.25**	SSH Protocol Version 1	22	**Medio**	The remote host is running a SSH server.This version supports connections made using version 1.33 and / or 1.5of the SSH protocol.These protocols should not be used since they are not completelycryptographically safe.		Use protocol 2 if you are using OpenSSH, if you are using SSH.com setthe option 'Ssh1Compatibility' to 'no'.	url - http://www.kb.cert.org/vuls/id/684820	CVE-2001-1473

10..**.25**	SSH Weak Ciphers	22	**Medio**	The remote SSH server allows communication with weak encryption ciphers. This may allow attackers to eavesdrop or disrupt communications. Note; A cipher is considered to be weak if it uses a small key length or has known published attacks against it.	---------- ---------- [Cipher] ---------- ---------- [arcfour]	If you are using SSH Communications Security's Secure Shell, configure it to use a stronger cipher such as AES128 using the 'SSH Secure Shell for Windows Server Configuration.' If you are using OpenSSH configure the Ciphers variable in /etc/sshd_config. See solution cross-references for configuration detail.	solution - http://www.ssh.com/support/documentation/online/ssh/winadminguide/32/Encryption.html solution - http://www.openbsd.org/cgi-bin/man.cgi?query=sshd_config&sektion=5	

10..**.25**	HTTP TRACE/TRACK Cross-Site Scripting Attack	80	**Medio**	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "cross-site tracing", when used in conjunction with various weaknesses in browsers. This is related to CVE-2004-2320 and CVE-2005-3398	Service responded to a TRACE request with the status code 200 and included our forged headers in the response	If the remote host is running Microsoft IIS, Use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. If the remote host is running Apache HTTP Daemon, Add the following lines for each virtual host in your configuration file: RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F]	solution - http://www.microsoft.com/technet/security/tools/urlscan.mspx solution - http://learn.iis.net/page.aspx/938/urlscan-3-reference/#UsingUrlScan	CVE-2007-3008

10..**.26**	SSH Protocol Version 1	22	**Medio**	The remote host is running a SSH server. This version supports connections made using version 1.33 and / or 1.5 of the SSH protocol. These protocols should not be used since they are not completely cryptographically safe.		Use protocol 2 if you are using OpenSSH, if you are using SSH.com set the option 'Ssh1Compatibility' to 'no'.	url - http://www.kb.cert.org/vuls/id/684820	CVE-2001-1473
10..**.26**	SSH Weak Ciphers	22	**Medio**	The remote SSH server allows communication with weak encryption ciphers. This may allow attackers to eavesdrop or disrupt communications.Note; A cipher is considered to be weak if it uses a small key length or has known published attacks against it.	----------[Cipher]----------[arcfour]	If you are using SSH Communications Security's Secure Shell, configure it to use a stronger cipher such as AES128 using the 'SSH Secure Shell for Windows Server Configuration.'If you are using OpenSSH configure the Ciphers variable in /etc/sshd_config .See solution cross-references for configuration detail.	solution - http://www.ssh.com/support/documentation/online/ssh/winadminguide/32/Encryption.htmlsolution - http://www.openbsd.org/cgi-bin/man.cgi?query=sshd_config&sektion=5	

10..**.26**	SSLv2 detected	443	**Medio**	An SSLv2 service is running on this port. Version 2 of the SSL protocol is vulnerable to several attacks and weaknesses The main attacks include a 'cipher downgrade' attack and a truncation 'attack'. The cipher downgrade attacks allows an attacker to force an already established session to use a weaker (easier to crack) cipher than originally negotiated. The truncation attack allows an attacker to stop a connection at an arbitrary point. It should be noted that, specifically, SSLv2 includes many weak ciphers and negotiates the ciphers in clear text.		Configure this service to only allow version 3 of the SSL protocol. Consult your product manual or vendor for information about how this is done.	url - http://www.educatedguesswork.org/movabletype/archives/2005/10/openssl_sslv2_r.html solution - http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslciphersuite solution - http://support.microsoft.com/kb/187498 solution - http://redmine.lighttpd.net/wiki/1/Docs:SSL#PCI-DSS-compliance solution - http://wiki.nginx.org/NginxHttpSslModule#ssl_ciphers	

10..**.26**	SSL/TLS Weak and Export Ciphers Detected	443	**Medio**	The service running on this port allows the use of weak encryption ciphers, which might allow an attacker to eavesdrop on the communication.	---------- [SSLv2 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RC4_128_EXPORT40_WITH_MD5][EXP-RC4-MD5][128][40][export] ---------- [SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RSA_EXPORT_WI	For Apache, add the following line to the configuration file (e.g. httpd.conf): SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM and restart the server. For Microsoft IIS, set the following registry keys to 0: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL	url - http://support.microsoft.com/default.aspx?scid=kb;en-us;245030 url - http://blog.stardothosting.com/2009/05/22/testing-for-weak-ssl-ciphers-for-security-audits/ url - http://www.routerzone.eu/wiki/index.php/Restricting_Weak_SSL_Ciphers,_F5_BigIP url - http://www.openssl.org/docs/apps/ciphers.html solution - http://blog.zenone.org/2009/03/pci-compliance-disable-sslv2-and-weak.html	

					TH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] ---------- [TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export]	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC240/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC256/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC440/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC456/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\C		

						iphers\RC4 64/128		

10..**.26**	Directory Browsing	80	**Medio**	This service lists the contents of various directories.	Browsable directories:---------- ---------- --[Location]---------- ---------- --[/tmp/]	Disable directory browsing		

10..**.26**	SSL Certificate Authenticity	443	**Medio**	The certificate presented by this service does not seem to have been issued by a valid Certificate Authority (CA). By having a trusted CA sign your certificate, they certify that you are in fact you. Note: This finding is issued if it is not possible to verify the authenticity of the certificate presented by the service, and is sometimes a result of the service being misconfigured. Any SSLv3/TLSv1 compliant service must present the complete chain of certificates used to sign its own, optionally excluding the root CA certificate. A more detailed reason for why the chain of trust was broken is listed in the table in the information section of this finding.	---------- [depth][country][state][locality][organization][common name][error] ---------- [0][US][MyServer State][MyServer Town][MyServer, Ltd][www.myserver.dom][unable to get local issuer certificate]	Use a valid Certificate Authority (CA)		

10..**.26**	SSL Certificate Name Mismatch	443	**Medio**	The SSL certificate used by this service is not valid for the domain name where this service is located. This could allow for man-in-the-middle attacks.	None of the subject common names (www.myserver.dom) match any of the following domains: svn.********.gob.mx and 10.**.**.26.	Using certificates with mismatched names is fine for development or testing servers but, for production servers a completely valid certificate should be used. If this host is a production server, you should purchase and install a server certificate signed by a trusted Certificate Authority. Ensure that the domain where the certificate is used matches the domain encoded in the certificate.	solution - http://www.digicert.com/ssl-support/certificate-name-mismatch-error.htm	

10..**.26**	SSL/TLS Cipher Suite Detect MD5	443	**Medio**	The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5 in the signature algorithm of an X.509 certificate.	----------[SSLv2 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength]---------- [RC4_128_WITH_MD5][RC4-MD5][128][128][medium][RC4_128_EXPORT40_WITH_MD5][EXP-RC4-MD5][128][40][export]----------[SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength]---------- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export][RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium]---------- [TLSv1 Cipher Suite][OpenSSL	Reconfigure the service to disallow the listed cipher suites	url - http://www.kb.cert.org/vuls/id/836068	CVE-2004-2761

					Cipher Name][Algorithm Bits][Bits Used][Cipher Strength]---------- ---------- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export][RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium]			
10..**.26**	HTTP TRACE/TRACK Cross-Site Scripting Attack	443	**Medio**	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "cross-site tracing", when used in conjunction with various weaknesses in browsers. This is related to CVE-2004-2320 and CVE-2005-3398	Service responded to a TRACE request with the status code 200 and included our forged headers in the response	If the remote host is running Microsoft IIS, Use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. If the remote host is running Apache HTTP Daemon, Add the following lines for each virtual host in your	solution - http://www.microsoft.com/technet/security/tools/urlscan.mspx solution - http://learn.iis.net/page.aspx/938/urlscan-3-reference/#UsingURLScan	CVE-2007-3008

						configuration file: RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* -[F]		

10..**.26**	HTTP TRACE/TRACK Cross-Site Scripting Attack	80	**Medio**	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "cross-site tracing", when used in conjunction with various weaknesses in browsers.This is related to CVE-2004-2320 and CVE-2005-3398	Service responded to a TRACE request with the status code 200 and included our forged headers in the response	If the remote host is running Microsoft IIS, Use the URLScan tool to deny HTTP TRACE requests or to permit only themethods needed to meet site requirements and policy.If the remote host is running Apache HTTP Daemon,Add the following lines for each virtual host in your configuration file:RewriteEngine onRewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)RewriteRule .* - [F]	solution - http://www.microsoft.com/technet/security/tools/urlscan.mspxsolution - http://learn.iis.net/page.aspx/938/urlscan-3-reference/#UsingUrlScan	CVE-2007-3008

10..*.2**	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability	445	**Medio**	Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.microsoft.com/	CVE-2007-1912

10..*.2**	SSLv2 detected	8098	**Medio**	An SSLv2 service is running on this port. Version 2 of the SSL protocol is vulnerable to several attacks and weaknesses The main attacks include a 'cipher downgrade' attack and a truncation 'attack'. The cipher downgrade attacks allows an attacker to force an already established session to use a weaker (easier to crack) cipher than originally negotiated. The truncation attack allows an attacker to stop a connection at an arbitrary point. It should be noted that, specifically, SSLv2 includes many weak ciphers and negotiates the ciphers in clear text.		Configure this service to only allow version 3 of the SSL protocol. Consult your product manual or vendor for information about how this is done.	url - http://www.educatedguesswork.org/movabletype/archives/2005/10/openssl_sslv2_r.html solution - http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslciphersuite solution - http://support.microsoft.com/kb/187498 solution - http://redmine.lighttpd.net/wiki/1/Docs:SSL#PCI-DSS-compliance solution - http://wiki.nginx.org/NginxHttpSslModule#ssl_ciphers	

10..*.2**	SSL/TLS Renegotiation Handshakes Man-in-the-Middle Plaintext Data Injection	8098	**Medio**	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS), mod_ssl in the Apache HTTP Server, OpenSSL, Mozilla Network Security Services (NSS), multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context.		OpenSSL has provided a fix for this in version 0.9.8m and later.Microsoft has released a workaround to disable renegotiation.	solution - http://www.openssl.org/source/solution - http://support.microsoft.com/kb/977377 solution - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555	CVE-2009-3555

10..*.2**	SSL/TLS Weak and Export Ciphers Detected	8098	**Medio**	The service running on this port allows the use of weak encryption ciphers, which might allow an attacker to eavesdrop on the communication.	---------- [SSLv2 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RC4_128_EXPORT40_WITH_MD5][EXP-RC4-MD5][128][40][export] [RC2_128_CBC_EXPORT40_WITH_MD5][EXP-RC2-CBC-MD5][128][40][export] [DES_64_CBC_WITH_MD5][DES-CBC-MD5][56][56][weak] ---------- ----------	For Apache, add the following line to the configuration file (e.g. httpd.conf): SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM and restart the server. For Microsoft IIS, set the following registry keys to 0: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL	url - http://support.microsoft.com/default.aspx?scid=kb;en-us;245030 url - http://blog.stardothosting.com/2009/05/22/testing-for-weak-ssl-ciphers-for-security-audits/ url - http://www.routerzone.eu/wiki/index.php/Restricting_Weak_SSL_Ciphers,_F5_BigIP url - http://www.openssl.org/docs/apps/ciphers.html solution - http://blog.zenone.org/2009/03/pci-compliance-disable-sslv2-and-weak.html	

					[SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] --- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export] [RSA_WITH_DES_CBC_SHA][DES-CBC-SHA][56][56][weak] [RSA_EXPORT1024_WITH_DES_CBC_SHA][EXP1024-DES-CBC-SHA][56][56][export] [RSA_EXPORT1024_WITH_RC4_56_	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\C		

					SHA][EXP1024-RC4-SHA][128][56][export] --- [TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] --- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export] [RSA_WITH_DES_CBC_SHA][DES-CBC-	iphers\RC4 64/128		

					SHA][56][56][weak] [RSA_EXPORT1024_WITH_DES_CBC_SHA][EXP1024-DES-CBC-SHA][56][56][export] [RSA_EXPORT1024_WITH_RC4_56_SHA][EXP1024-RC4-SHA][128][56][export			

10..*.2**	SSL Certificate Authenticity	8098	**Medio**	The certificate presented by this service does not seem to have been issued by a valid Certificate Authority (CA). By having a trusted CA sign your certificate, they certify that you are in fact you. Note: This finding is issued if it is not possible to verify the authenticity of the certificate presented by the service, and is sometimes a result of the service being misconfigured. Any SSLv3/TLSv1 compliant service must present the complete chain of certificates used to sign its own, optionally excluding the root CA certificate. A more detailed reason for why the chain of trust was broken is listed in the table in the information section of this finding.	---------- [depth][country][state][locality][organization][common name][error] ---------- [0][][][][][antivirus.ad.gob][self signed certificate]	Use a valid Certificate Authority (CA)		

10..*.2**	SSL/TLS Cipher Suite Detect MD5	8098	**Medio**	The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5 in the signature algorithm of an X.509 certificate.	----------[SSLv2 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength]----------[RC4_128_WITH_MD5][RC4-MD5][128][128][medium][RC4_128_EXPORT40_WITH_MD5][EXP-RC4-MD5][128][40][export][RC2_128_CBC_WITH_MD5][RC2-CBC-MD5][128][128][medium][RC2_128_CBC_EXPORT40_WITH_MD5][EXP-RC2-CBC-MD5][128][40][export][DES_64_CBC_WITH_MD5][DES-CBC-MD5][56][56][weak][DES_192_EDE3_CBC_WITH_MD5][DES-CBC3-MD5][168][168][strong]----------[SSLv3 Cipher Suite][OpenSSL	Reconfigure the service to disallow the listed cipher suites	url - http://www.kb.cert.org/vuls/id/836068	CVE-2004-2761

					Cipher Name][Algorithm Bits][Bits Used][Cipher Strength]----------[RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export][RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium][RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export]----------[TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength]----------[RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export][RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium][RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-			

					RC2-CBC-MD5][128][40][export]			

10..*.2**	SSL Certificate Name Mismatch	8098	**Medio**	The SSL certificate used by this service is not valid for the domain name where this service is located. This could allow for man-in-the-middle attacks.	None of the subject common names (antivirus.ad.gob, antivirus and antivirus.ad.gob) match any of the following domains: 10.**.*.2.	Using certificates with mismatched names is fine for development or testing servers but, for production servers a completely valid certificate should be used. If this host is a production server, you should purchase and install a server certificate signed by a trusted Certificate Authority. Ensure that the domain where the certificate is used matches the domain encoded in the certificate.	solution - http://www.digicert.com/ssl-support/certificate-name-mismatch-error.htm	

10..*.2**	Microsoft Windows: PostMessage function with 0x4c value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x4c value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1735
10..*.2**	Microsoft Windows: PostMessage function with 0x18d value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x18d value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1734

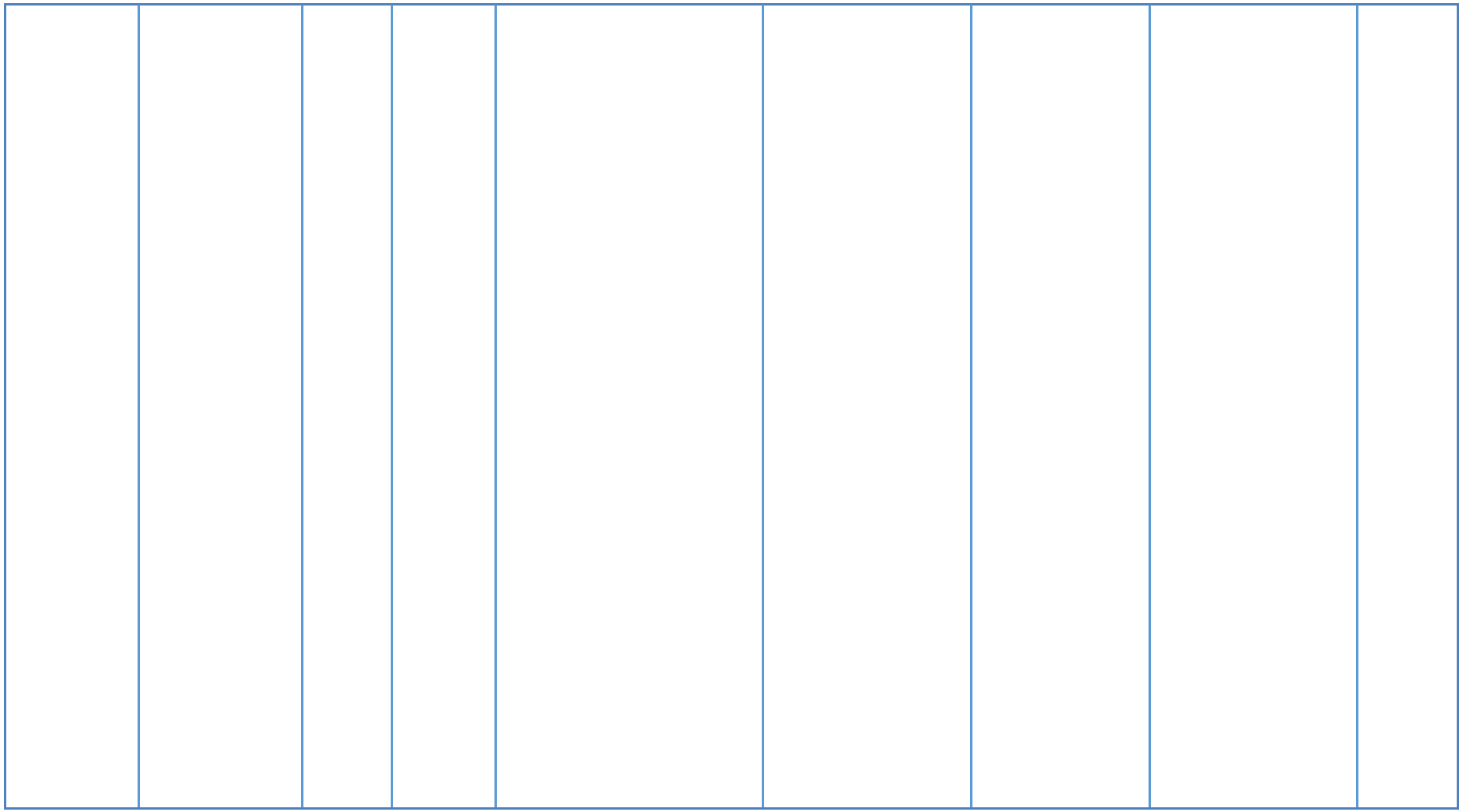
10..*.2**	Microsoft Windows: Unspecified API Argument Validation Local DoS	445	**Medio**	An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-0719
10..*.3**	Unencrypted Remote Authentication Available - Telnet	23	**Medio**	This telnet service allows cleartext or very weak authentication protocols without any encryption encapsulating login sessions.		Switch to SSH, if you need shell access to this host. Otherwise, disable/filter access to this Telnet service.		
10..*.3**	SSH Protocol Version 1	22	**Medio**	The remote host is running a SSH server. This version supports connections made using version 1.33 and / or 1.5 of the SSH protocol. These protocols should not be used since they are not completely cryptographically safe.		Use protocol 2 if you are using OpenSSH, if you are using SSH.com set the option 'Ssh1Compatibility' to 'no'.	url - http://www.kb.cert.org/vuls/id/684820	CVE-2001-1473

10..*.3**	SSH Weak Ciphers	22	**Medio**	The remote SSH server allows communication with weak encryption ciphers. This may allow attackers to eavesdrop or disrupt communications. Note; A cipher is considered to be weak if it uses a small key length or has known published attacks against it.	---------- ---------- [Cipher] ---------- ---------- [arcfour]	If you are using SSH Communications Security's Secure Shell, configure it to use a stronger cipher such as AES128 using the 'SSH Secure Shell for Windows Server Configuration.' If you are using OpenSSH configure the Ciphers variable in /etc/sshd_config. See solution cross-references for configuration detail.	solution - http://www.ssh.com/support/documentation/online/ssh/winadminguide/32/Encryption.html solution - http://www.openbsd.org/cgi-bin/man.cgi?query=sshd_config&sektion=5	

10..*.3**	SSL/TLS Renegotiation Handshakes Man-in-the-Middle Plaintext Data Injection	5307	**Medio**	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS), mod_ssl in the Apache HTTP Server, OpenSSL, Mozilla Network Security Services (NSS), multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context.		OpenSSL has provided a fix for this in version 0.9.8m and later. Microsoft has released a workaround to disable renegotiation.	solution - http://www.openssl.org/source/ solution - http://support.microsoft.com/kb/977377 solution - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555	CVE-2009-3555

10..*.3**	SSL Certificate Authenticity	5307	**Medio**	The certificate presented by this service does not seem to have beenissued by a valid Certificate Authority (CA). By having a trusted CAsign your certificate, they certify that you are in fact you.Note: This finding is issued if it is not possible to verify the authenticityof the certificate presented by the service, and is sometimes a result of theservice being misconfigured. Any SSLv3/TLSv1 compliant service must presentthe complete chain of certificates used to sign its own, optionally excluding the root CA certificate. A more detailed reason for why the chain of trustwas broken is listed in the table in the information section of this finding.	----------[depth][country][state][locality][organization][common name][error]----------[0][][][][][**********.*********.gob.mx][][1][][][][][**********.*********.gob.mx CA Cert][self signed certificate in certificate chain]	Use a valid Certificate Authority (CA)		

10..*.3**	SSL/TLS Cipher Suite Detect MD5	5307	**Medio**	The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5 in the signature algorithm of an X.509 certificate.	---------- [SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium] [TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium]	Reconfigure the service to disallow the listed cipher suites	url - http://www.kb.cert.org/vuls/id/836068	CVE-2004-2761



10..*.3**	HTTP TRACE/TRACK Cross-Site Scripting Attack	80	**Medio**	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "cross-site tracing", when used in conjunction with various weaknesses in browsers. This is related to CVE-2004-2320 and CVE-2005-3398	Service responded to a TRACE request with the status code 200 and included our forged headers in the response	If the remote host is running Microsoft IIS, Use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. If the remote host is running Apache HTTP Daemon, Add the following lines for each virtual host in your configuration file: RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F]	solution - http://www.microsoft.com/technet/security/tools/urlscan.mspx solution - http://learn.iis.net/page.aspx/938/urlscan-3-reference/#UsingURLScan	CVE-2007-3008

10..*.4**	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability	445	**Medio**	Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.microsoft.com/	CVE-2007-1912

10..*.4**	SSLv2 detected	636	**Medio**	An SSLv2 service is running on this port. Version 2 of the SSL protocol is vulnerable to several attacks and weaknesses The main attacks include a 'cipher downgrade' attack and a truncation 'attack'. The cipher downgrade attacks allows an attacker to force an already established session to use a weaker (easier to crack) cipher than originally negotiated. The truncation attack allows an attacker to stop a connection at an arbitrary point. It should be noted that, specifically, SSLv2 includes many weak ciphers and negotiates the ciphers in clear text.		Configure this service to only allow version 3 of the SSL protocol. Consult your product manual or vendor for information about how this is done.	url - http://www.educatedguesswork.org/movabletype/archives/2005/10/openssl_sslv2_r.html solution - http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslciphersuite solution - http://support.microsoft.com/kb/187498 solution - http://redmine.lighttpd.net/wiki/1/Docs:SSL#PCI-DSS-compliance solution - http://wiki.nginx.org/NginxHttpSslModule#ssl_ciphers	

10..*.4**	SSLv2 detected	3269	**Medio**	An SSLv2 service is running on this port. Version 2 of the SSL protocol is vulnerable to several attacks and weaknesses The main attacks include a 'cipher downgrade' attack and a truncation 'attack'. The cipher downgrade attacks allows an attacker to force an already established session to use a weaker (easier to crack) cipher than originally negotiated. The truncation attack allows an attacker to stop a connection at an arbitrary point. It should be noted that, specifically, SSLv2 includes many weak ciphers and negotiates the ciphers in clear text.		Configure this service to only allow version 3 of the SSL protocol. Consult your product manual or vendor for information about how this is done.	url - http://www.educatedguesswork.org/movabletype/archives/2005/10/openssl_sslv2_r.html solution - http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslciphersuite solution - http://support.microsoft.com/kb/187498 solution - http://redmine.lighttpd.net/wiki/1/Docs:SSL#PCI-DSS-compliance solution - http://wiki.nginx.org/NginxHttpSslModule#ssl_ciphers	

10..*.4**	SSL/TLS Renegotiation Handshakes Man-in-the-Middle Plaintext Data Injection	636	**Medio**	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS), mod_ssl in the Apache HTTP Server, OpenSSL, Mozilla Network Security Services (NSS), multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context.		OpenSSL has provided a fix for this in version 0.9.8m and later. Microsoft has released a workaround to disable renegotiation.	solution - http://www.openssl.org/source/ solution - http://support.microsoft.com/kb/977377 solution - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555	CVE-2009-3555

10..*.4**	SSL/TLS Renegotiation Handshakes Man-in-the-Middle Plaintext Data Injection	3269	**Medio**	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS), mod_ssl in the Apache HTTP Server, OpenSSL, Mozilla Network Security Services (NSS), multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context.		OpenSSL has provided a fix for this in version 0.9.8m and later.Microsoft has released a workaround to disable renegotiation.	solution - http://www.openssl.org/source/solution - http://support.microsoft.com/kb/977377 solution - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555	CVE-2009-3555

10..*.4**	SSL/TLS Weak and Export Ciphers Detected	636	**Medio**	The service running on this port allows the use of weak encryption ciphers, which might allow an attacker to eavesdrop on the communication.	---------- [SSLv2 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RC4_128_EXPORT40_WITH_MD5][EXP-RC4-MD5][128][40][export] [RC2_128_CBC_EXPORT40_WITH_MD5][EXP-RC2-CBC-MD5][128][40][export] [DES_64_CBC_WITH_MD5][DES-CBC-MD5][56][56][weak] ---------- ----------	For Apache, add the following line to the configuration file (e.g. httpd.conf): SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM and restart the server. For Microsoft IIS, set the following registry keys to 0: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL	url - http://support.microsoft.com/default.aspx?scid=kb;en-us;245030 url - http://blog.stardothosting.com/2009/05/22/testing-for-weak-ssl-ciphers-for-security-audits/ url - http://www.routerzone.eu/wiki/index.php/Restricting_Weak_SSL_Ciphers,_F5_BigIP url - http://www.openssl.org/docs/apps/ciphers.html solution - http://blog.zenone.org/2009/03/pci-compliance-disable-sslv2-and-weak.html	

					[SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] --- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export] [RSA_WITH_DES_CBC_SHA][DES-CBC-SHA][56][56][weak] [RSA_EXPORT1024_WITH_DES_CBC_SHA][EXP1024-DES-CBC-SHA][56][56][export] [RSA_EXPORT1024_WITH_RC4_56_	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\C		

					SHA][EXP1024-RC4-SHA][128][56][export] --- [TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] --- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export] [RSA_WITH_DES_CBC_SHA][DES-CBC-	iphers\RC4 64/128		

					SHA][56][56][weak] [RSA_EXPORT1024_WITH_DES_CBC_SHA][EXP1024-DES-CBC-SHA][56][56][export] [RSA_EXPORT1024_WITH_RC4_56_SHA][EXP1024-RC4-SHA][128][56][export]			

10..*.4**	SSL/TLS Weak and Export Ciphers Detected	3269	**Medio**	The service running on this port allows the use of weak encryption ciphers, which might allow an attacker to eavesdrop on the communication.	---------- [SSLv2 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RC4_128_EXPORT40_WITH_MD5][EXP-RC4-MD5][128][40][export] [RC2_128_CBC_EXPORT40_WITH_MD5][EXP-RC2-CBC-MD5][128][40][export] [DES_64_CBC_WITH_MD5][DES-CBC-MD5][56][56][weak] ---------- ----------	For Apache, add the following line to the configuration file (e.g. httpd.conf): SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM and restart the server. For Microsoft IIS, set the following registry keys to 0: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL	url - http://support.microsoft.com/default.aspx?scid=kb;en-us;245030 url - http://blog.stardothosting.com/2009/05/22/testing-for-weak-ssl-ciphers-for-security-audits/ url - http://www.routerzone.eu/wiki/index.php/Restricting_Weak_SSL_Ciphers,_F5_BigIP url - http://www.openssl.org/docs/apps/ciphers.html solution - http://blog.zenone.org/2009/03/pci-compliance-disable-sslv2-and-weak.html	

					[SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] --- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export] [RSA_WITH_DES_CBC_SHA][DES-CBC-SHA][56][56][weak] [RSA_EXPORT1024_WITH_DES_CBC_SHA][EXP1024-DES-CBC-SHA][56][56][export] [RSA_EXPORT1024_WITH_RC4_56_	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\C		

					SHA][EXP1024-RC4-SHA][128][56][export] --- [TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] --- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export] [RSA_WITH_DES_CBC_SHA][DES-CBC-	iphers\RC4 64/128		

					SHA][56][56][weak] [RSA_EXPORT1024_WITH_DES_CBC_SHA][EXP1024-DES-CBC-SHA][56][56][export] [RSA_EXPORT1024_WITH_RC4_56_SHA][EXP1024-RC4-SHA][128][56][export]			

10..*.4**	DNS recursive queries	53	**Medio**	This DNS appears to allow recursive queries (i.e. requests for lookupsof third party names).In other words, anyone may request a lookup of any domain name. An attacker can take advantage of this problem to perform cache poisoning attacks againstthis nameserver.If the DNS allows recursive queries over UDP, this host can potentially alsobe used to 'bounce' denial of service attacks against other networks or systems.Note: If this nameserver is your internal nameserver, and the scan was performedfrom within your network, you may disregard this notice.		Restrict recursive queries to the hosts that should use this nameserver,such as those of the LAN connected to it.If you are using a Microsoft DNS sever, follow the applicable instructionsat the following URL: http://www.eukhost.com/forums/archive/index.php/t-852.htmlIf you are using bind 8, this can be done by using the instruction'allow-recursion' in the 'options' section of your 'named.conf'.If you are using bind 9, you can define a grouping of internal addressesusing the 'acl' command.Then, within the	url - http://www.subneural.net/files/bind9arm.pdfurl - http://technet2.microsoft.com/WindowsServer/en/library/e1fe9dff-e87b-44ae-ac82-8e76d19d9c371033.mspx	

						options block, you can explicitly state: allow-recursion {hosts_defined_in_acl}'If you are using another name server, consult its documentation.		

10..*.4**	DNS recursive queries	53	**Medio**	This DNS appears to allow recursive queries (i.e. requests for lookups of third party names). In other words, anyone may request a lookup of any domain name. An attacker can take advantage of this problem to perform cache-poisoning attacks against this nameserver. If the DNS allows recursive queries over UDP, this host can potentially also be used to 'bounce' denial of service attacks against other networks or systems. Note: If this nameserver is your internal nameserver, and the scan was performed from within your network, you may disregard this notice.		Restrict recursive queries to the hosts that should use this nameserver, such as those of the LAN connected to it. If you are using a Microsoft DNS sever, follow the applicable instructions at the following URL: http://www.eukhost.com/forums/archive/index.php/t-852.html If you are using bind 8, this can be done by using the instruction 'allow-recursion' in the 'options' section of your 'named.conf'. If you are using bind 9, you can define a grouping of internal addresses using the 'acl'	url - http://www.subneural.net/files/bind9arm.pdf url - http://technet2.microsoft.com/WindowsServer/en/library/e1fe9dff-e87b-44ae-ac82-8e76d19d9c371033.mspx	

						command. Then, within the options block, you can explicitly state: allow-recursion {hosts_defined_in_acl}' If you are using another name server, consult its documentation.		

10..*.4**	SSL Certificate Authenticity	636	**Medio**	The certificate presented by this service does not seem to have been issued by a valid Certificate Authority (CA). By having a trusted CA sign your certificate, they certify that you are in fact you. Note: This finding is issued if it is not possible to verify the authenticity of the certificate presented by the service, and is sometimes a result of the service being misconfigured. Any SSLv3/TLSv1 compliant service must present the complete chain of certificates used to sign its own, optionally excluding the root CA certificate. A more detailed reason for why the chain of trust was broken is listed in the table in the information section of this finding.	---------- [depth][country][state][locality][organization][common name][error] ---------- [0][][][][][********.ad.gob][unable to get local issuer certificate]	Use a valid Certificate Authority (CA)		

10..*.4**	SSL Certificate Authenticity	3269	**Medio**	The certificate presented by this service does not seem to have beenissued by a valid Certificate Authority (CA). By having a trusted CAsign your certificate, they certify that you are in fact you.Note: This finding is issued if it is not possible to verify the authenticityof the certificate presented by the service, and is sometimes a result of theservice being misconfigured. Any SSLv3/TLSv1 compliant service must presentthe complete chain of certificates used to sign its own, optionally excluding the root CA certificate. A more detailed reason for why the chain of trustwas broken is listed in the table in the information section of this finding.	----------[depth][country][state][locality][organization][common name][error]----------[0][][][][][********.ad.gob][unable to get local issuer certificate]	Use a valid Certificate Authority (CA)		

10..*.4**	SSL/TLS Cipher Suite Detect MD5	636	**Medio**	The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5 in the signature algorithm of an X.509 certificate.	---------- [SSLv2 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RC4_128_WITH_MD5][RC4-MD5][128][128][medium] [RC4_128_EXPORT40_WITH_MD5][EXP-RC4-MD5][128][40][export] [RC2_128_CBC_WITH_MD5][RC2-CBC-MD5][128][128][medium] [RC2_128_CBC_EXPORT40_WITH_MD5][EXP-RC2-CBC-MD5][128][40][export]	Reconfigure the service to disallow the listed cipher suites	url - http://www.kb.cert.org/vuls/id/836068	CVE-2004-2761

					[DES_64_CBC_WITH_MD5][DES-CBC-MD5][56][56][weak] [DES_192_EDE3_CBC_WITH_MD5][DES-CBC3-MD5][168][168][strong] ---------- [SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export]			

					---------- [TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export]			

10..*.4**	SSL/TLS Cipher Suite Detect MD5	3269	Medio	The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5 in the signature algorithm of an X.509 certificate.	[SSLv2 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RC4_128_WITH_MD5][RC4-MD5][128][128][medium] [RC4_128_EXPORT40_WITH_MD5][EXP-RC4-MD5][128][40][export] [RC2_128_CBC_WITH_MD5][RC2-CBC-MD5][128][128][medium] [RC2_128_CBC_EXPORT40_WITH_MD5][EXP-RC2-CBC-MD5][128][40][export] [DES_64_CBC_WITH_MD5][DES-CBC-	Reconfigure the service to disallow the listed cipher suites	url - http://www.kb.cert.org/vuls/id/836068	CVE-2004-2761

					MD5][56][56][weak] [DES_192_EDE3_CBC_WITH_MD5][DES-CBC3-MD5][168][168][strong] ---------- [SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export]			

					---------- [TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export]			

10..*.4**	Microsoft Windows: PostMessage function with 0x4c value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x4c value as the second argument.Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1735
10..*.4**	Microsoft Windows: PostMessage function with 0x18d value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x18d value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1734

10..*.4**	Microsoft Windows: Unspecified API Argument Validation Local DoS	445	**Medio**	An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-0719
10..*.5**	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability	445	**Medio**	Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.microsoft.com/	CVE-2007-1912

10..*.5**	Unencrypted Remote Authentication Available - POP3	110	**Medio**	This POP3 service allows cleartext or very weak authentication protocols without any encryption encapsulating login sessions.		POP3 can be secured by disabling cleartext authentication mechanisms, or by wrapping it in SSL/TLS. If the service is not required to be running, however, disable/filter access to it.		

10..*.5**	SSLv2 detected	443	**Medio**	An SSLv2 service is running on this port. Version 2 of the SSL protocol is vulnerable to several attacks and weaknesses The main attacks include a 'cipher downgrade' attack and a truncation 'attack'. The cipher downgrade attacks allows an attacker to force an already established session to use a weaker (easier to crack) cipher than originally negotiated. The truncation attack allows an attacker to stop a connection at an arbitrary point. It should be noted that, specifically, SSLv2 includes many weak ciphers and negotiates the ciphers in clear text.		Configure this service to only allow version 3 of the SSL protocol. Consult your product manual or vendor for information about how this is done.	url - http://www.educatedguesswork.org/movabletype/archives/2005/10/openssl_sslv2_r.html solution - http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslciphersuite solution - http://support.microsoft.com/kb/187498 solution - http://redmine.lighttpd.net/wiki/1/Docs:SSL#PCI-DSS-compliance solution - http://wiki.nginx.org/NginxHttpSslModule#ssl_ciphers	

10..*.5**	SSL/TLS Weak and Export Ciphers Detected	443	**Medio**	The service running on this port allows the use of weak encryption ciphers, which might allow an attacker to eavesdrop on the communication.	----------[SSLv2 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength]----------[RC4_128_EXPORT40_WITH_MD5][EXP-RC4-MD5][128][40][export][RC2_128_CBC_EXPORT40_WITH_MD5][EXP-RC2-CBC-MD5][128][40][export][DES_64_CBC_WITH_MD5][DES-CBC-MD5][56][56][weak]----------[SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength]----------[RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export][RSA_EXPORT_	For Apache, add the following line to the configuration file (e.g. httpd.conf):SSL CipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUMand restart the server.For Microsoft IIS, set the following registry keys to 0:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULLHKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128HKEY_L	url - http://support.microsoft.com/default.aspx?scid=kb;en-us;245030url - http://blog.stardothosting.com/2009/05/22/testing-for-weak-ssl-ciphers-for-security-audits/url - http://www.routerzone.eu/wiki/index.php/Restricting_Weak_SSL_Ciphers,_F5_BigIPurl - http://www.openssl.org/docs/apps/ciphers.htmlsolution - http://blog.zenone.org/2009/03/pci-compliance-disable-sslv2-and-weak.html	

					WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export][RSA_WITH_DES_CBC_SHA][DES-CBC-SHA][56][56][weak][RSA_EXPORT1024_WITH_DES_CBC_SHA][EXP1024-DES-CBC-SHA][56][56][export][RSA_EXPORT1024_WITH_RC4_56_SHA][EXP1024-RC4-SHA][128][56][export]----------[TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength]----------[RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export][RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export][RSA_WITH_DE	OCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128		

					S_CBC_SHA][DES-CBC-SHA][56][56][weak][RSA_EXPORT1024_WITH_DES_CBC_SHA][EXP1024-DES-CBC-SHA][56][56][export][RSA_EXPORT1024_WITH_RC4_56_SHA][EXP1024-RC4-SHA][128][56][export]			

10..*.5**	SSL/TLS Weak and Export Ciphers Detected	995	**Medio**	The service running on this port allows the use of weak encryption ciphers, which might allow an attacker to eavesdrop on the communication.	---------- ---------- [SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- ---------- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export] [RSA_WITH_DES_CBC_SHA][DES-CBC-SHA][56][56][weak] [RSA_EXPORT1024_WITH_DES_CBC_SHA][EXP1024-DES-CBC-SHA][56][56][export]	For Apache, add the following line to the configuration file (e.g. httpd.conf): SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM and restart the server. For Microsoft IIS, set the following registry keys to 0: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL	url - http://support.microsoft.com/default.aspx?scid=kb;en-us;245030 url - http://blog.stardothosting.com/2009/05/22/testing-for-weak-ssl-ciphers-for-security-audits/ url - http://www.routerzone.eu/wiki/index.php/Restricting_Weak_SSL_Ciphers,_F5_BigIP url - http://www.openssl.org/docs/apps/ciphers.html solution - http://blog.zenone.org/2009/03/pci-compliance-disable-sslv2-and-weak.html	

					[RSA_EXPORT1024_WITH_RC4_56_SHA][EXP1024-RC4-SHA][128][56][export] ---------- [TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export]	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\C		

					[RSA_WITH_DES_CBC_SHA][DES-CBC-SHA][56][56][weak] [RSA_EXPORT1024_WITH_DES_CBC_SHA][EXP1024-DES-CBC-SHA][56][56][export] [RSA_EXPORT1024_WITH_RC4_56_SHA][EXP1024-RC4-SHA][128][56][export]	iphers\RC4 64/128		

10..*.5**	SSL Certificate Authenticity	443	**Medio**	The certificate presented by this service does not seem to have been issued by a valid Certificate Authority (CA). By having a trusted CA sign your certificate, they certify that you are in fact you. Note: This finding is issued if it is not possible to verify the authenticity of the certificate presented by the service, and is sometimes a result of the service being misconfigured. Any SSLv3/TLSv1 compliant service must present the complete chain of certificates used to sign its own, optionally excluding the root CA certificate. A more detailed reason for why the chain of trust was broken is listed in the table in the information section of this finding.	---------- [depth][country][state][locality][organization][common name][error] ---------- [0][MX][Distrito Federal][Mexico][**********r][correo.**********.gob.mx][unable to get local issuer certificate]	Use a valid Certificate Authority (CA)		

10..*.5**	SSL Certificate Authenticity	995	**Medio**	The certificate presented by this service does not seem to have beenissued by a valid Certificate Authority (CA). By having a trusted CAsign your certificate, they certify that you are in fact you.Note: This finding is issued if it is not possible to verify the authenticityof the certificate presented by the service, and is sometimes a result of theservice being misconfigured. Any SSLv3/TLSv1 compliant service must presentthe complete chain of certificates used to sign its own, optionally excluding the root CA certificate. A more detailed reason for why the chain of trustwas broken is listed in the table in the information section of this finding.	----------[depth][country][state][locality][organization][common name][error]----------[0][MX][Distrito Federal][Mexico][**********.gob.mx][unable to get local issuer certificate]	Use a valid Certificate Authority (CA)		

10..*.5**	SSL/TLS Cipher Suite Detect MD5	443	**Medio**	The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5 in the signature algorithm of an X.509 certificate.	---------- [SSLv2 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RC4_128_WITH_MD5][RC4-MD5][128][128][medium] [RC4_128_EXPORT40_WITH_MD5][EXP-RC4-MD5][128][40][export] [RC2_128_CBC_WITH_MD5][RC2-CBC-MD5][128][128][medium] [RC2_128_CBC_EXPORT40_WITH_MD5][EXP-RC2-CBC-MD5][128][40][export]	Reconfigure the service to disallow the listed cipher suites	url - http://www.kb.cert.org/vuls/id/836068	CVE-2004-2761

					[DES_64_CBC_WITH_MD5][DES-CBC-MD5][56][56][weak] [DES_192_EDE3_CBC_WITH_MD5][DES-CBC3-MD5][168][168][strong] --- [SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] --- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium]			

					[RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export] --- [TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] --- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium] [RSA_EXPORT_WITH_RC2_CBC_40_			

					MD5][EXP-RC2-CBC-MD5][128][40][export]			

10..*.5**	SSL/TLS Cipher Suite Detect MD5	995	**Medio**	The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5 in the signature algorithm of an X.509 certificate.	---------- [SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] ---------- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export] ----------	Reconfigure the service to disallow the listed cipher suites	url - http://www.kb.cert.org/vuls/id/836068	CVE-2004-2761

					[TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] --- [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium] [RSA_EXPORT_WITH_RC2_CBC_40_MD5][EXP-RC2-CBC-MD5][128][40][export]			

10..*.5**	Microsoft Windows: PostMessage function with 0x4c value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x4c value as the second argument.Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1735
10..*.5**	Microsoft Windows: PostMessage function with 0x18d value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x18d value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1734

10..*.5**	Microsoft Windows: Unspecified API Argument Validation Local DoS	445	**Medio**	An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-0719
10..*.1**	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability	445	**Medio**	Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://www.microsoft.com/	CVE-2007-1912

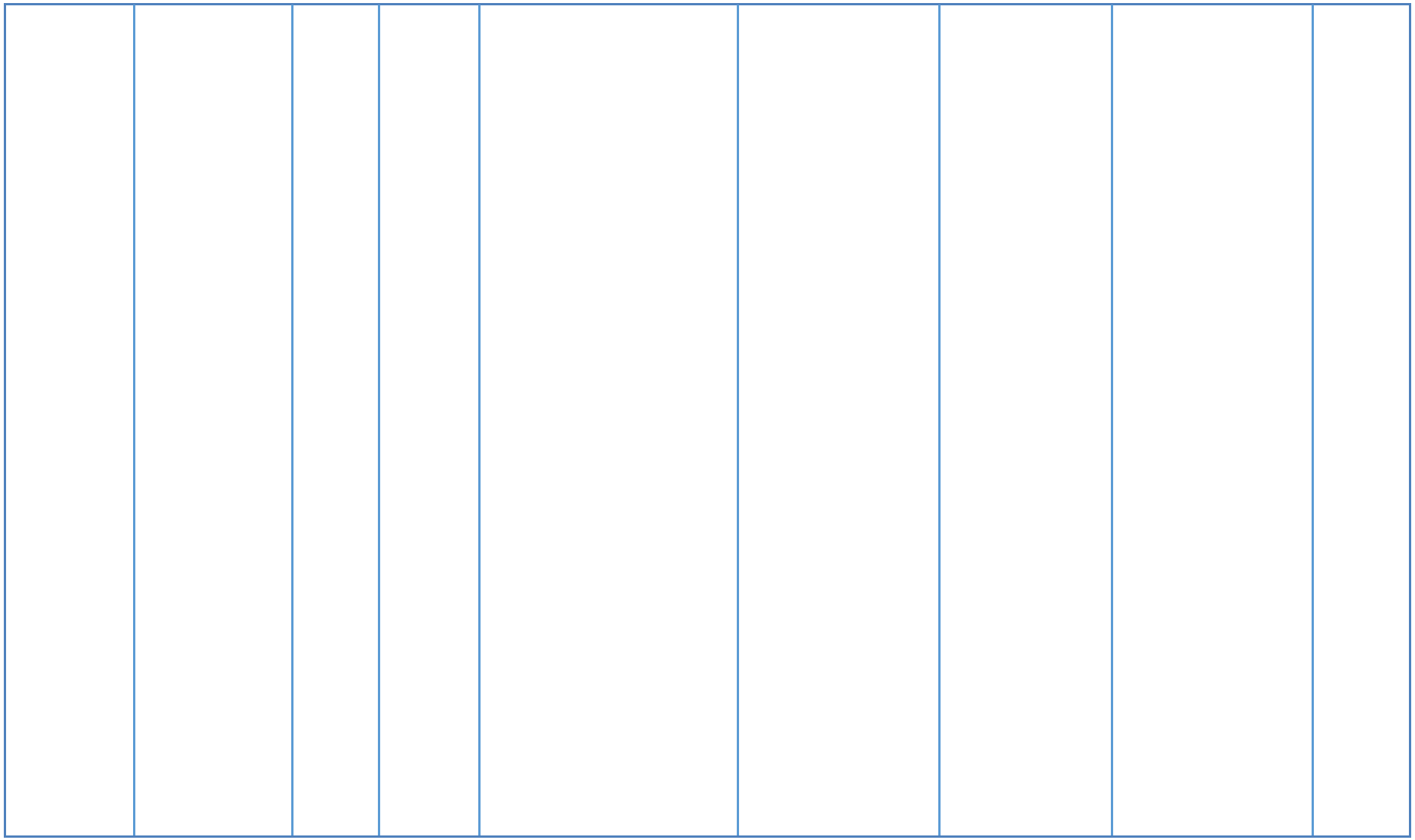
10..*.1**	SSL/TLS Renegotiation Handshakes Man-in-the-Middle Plaintext Data Injection	1311	**Medio**	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS), mod_ssl in the Apache HTTP Server, OpenSSL, Mozilla Network Security Services (NSS), multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context.		OpenSSL has provided a fix for this in version 0.9.8m and later. Microsoft has released a workaround to disable renegotiation.	solution - http://www.openssl.org/source/ solution - http://support.microsoft.com/kb/977377 solution - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555	CVE-2009-3555

10..*.1**	SSL/TLS Weak and Export Ciphers Detected	1311	**Medio**	The service running on this port allows the use of weak encryption ciphers, which might allow an attacker to eavesdrop on the communication.	----------[SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength]----------[RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export][RSA_WITH_DES_CBC_SHA][DES-CBC-SHA][56][56][weak]----------[TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength]----------[RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export][RSA_WITH_DES_CBC_SHA][DES-CBC-SHA][56][56][weak]	For Apache, add the following line to the configuration file (e.g. httpd.conf):SSL CipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUMand restart the server.For Microsoft IIS, set the following registry keys to 0:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULLHKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128HKEY_L	url - http://support.microsoft.com/default.aspx?scid=kb;en-us;245030url - http://blog.stardothosting.com/2009/05/22/testing-for-weak-ssl-ciphers-for-security-audits/url - http://www.routerzone.eu/wiki/index.php/Restricting_Weak_SSL_Ciphers,_F5_BigIPurl - http://www.openssl.org/docs/apps/ciphers.htmlsolution - http://blog.zenone.org/2009/03/pci-compliance-disable-sslv2-and-weak.html	

						OCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128		

10..*.1**	SSL Certificate Authenticity	1311	**Medio**	The certificate presented by this service does not seem to have been issued by a valid Certificate Authority (CA). By having a trusted CA sign your certificate, they certify that you are in fact you. Note: This finding is issued if it is not possible to verify the authenticity of the certificate presented by the service, and is sometimes a result of the service being misconfigured. Any SSLv3/TLSv1 compliant service must present the complete chain of certificates used to sign its own, optionally excluding the root CA certificate. A more detailed reason for why the chain of trust was broken is listed in the table in the information section of this finding.	---------- ---------- [depth][country][state][locality][organization][common name][error] ---------- ---------- [0][][TX c=US][Round Rock][Dell Inc][SERVER1][self signed certificate]	Use a valid Certificate Authority (CA)		

10..*.1**	SSL/TLS Cipher Suite Detect MD5	1311	**Medio**	The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5 in the signature algorithm of an X.509 certificate.	[SSLv3 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium] [TLSv1 Cipher Suite][OpenSSL Cipher Name][Algorithm Bits][Bits Used][Cipher Strength] [RSA_EXPORT_WITH_RC4_40_MD5][EXP-RC4-MD5][128][40][export] [RSA_WITH_RC4_128_MD5][RC4-MD5][128][128][medium]	Reconfigure the service to disallow the listed cipher suites	url - http://www.kb.cert.org/vuls/id/836068	CVE-2004-2761



10..*.1**	SSL Certificate Name Mismatch	1311	**Medio**	The SSL certificate used by this service is not valid for the domain name where this service is located. This could allow for man-in-the-middle attacks.	None of the subject common names (SERVER1) match any of the following domains: server1.ad.gob and 10. **.*.1.	Using certificates with mismatched names is fine for development or testing servers but for production servers a completely valid certificate should be used. If thishost is a production server, you should purchase and install a server certificatesigned by a trusted Certificate Authority. Ensure that the domain where the certificate is usedmatches the domain encoded in the certificate.	solution - http://www.digicert.com/ssl-support/certificate-name-mismatch-error.htm	

10..*.1**	Microsoft Windows: PostMessage function with 0x4c value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x4c value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1735
10..*.1**	Microsoft Windows: PostMessage function with 0x18d value causes DoS of win32k.sys	445	**Medio**	Local attackers can use the PostMessage function call to generate a win32k.sys error causing a denial of service (system crash) by passing a 0x18d value as the second argument. Currently the only solution is to restrict local access to trusted users only.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Upgrade to the latest version of Microsoft Windows.	url - http://microsoft.com/windows	CVE-2010-1734

10..*.1**	Microsoft Windows: Unspecified API Argument Validation Local DoS	445	**Medio**	An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.	This vulnerability was identified because (1) the version of Microsoft Windows, 5.2 sp2, is less than or equal to 5.2 SP2.	The vendor has not acknowledged the existence of this vulnerability. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime	url - http://microsoft.com/windows	CVE-2010-0719

10..*.1**	HTTP TRACE/TRACK Cross-Site Scripting Attack	1311	**Medio**	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods, which are used to debug web server connections.It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "cross-site tracing", when used in conjunction with various weaknesses in browsers.This is related to CVE-2004-2320 and CVE-2005-3398	Service responded to a TRACE request with the status code 200Service responded to a TRACK request with the status code 200	If the remote host is running Microsoft IIS, Use the URLScan tool to deny HTTP TRACE requests or to permit only themethods needed to meet site requirements and policy.If the remote host is running Apache HTTP Daemon,Add the following lines for each virtual host in your configuration file:RewriteEngine onRewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)RewriteRule .* - [F]	solution - http://www.microsoft.com/technet/security/tools/urlscan.mspxsolution - http://learn.iis.net/page.aspx/938/urlscan-3-reference/#UsingUrlScan	CVE-2007-3008

10..*.6**	SSH Weak Ciphers	22	**Medio**	The remote SSH server allows communication with weak encryption ciphers. This may allow attackers to eavesdrop or disrupt communications. Note; A cipher is considered to be weak if it uses a small key length or has known published attacks against it.	---------- [Cipher] ---------- [des] [none] [arcfour]	If you are using SSH Communications Security's Secure Shell, configure it to use a stronger cipher such as AES128 using the 'SSH Secure Shell for Windows Server Configuration.' If you are using OpenSSH, configure the Ciphers variable in /etc/sshd_config. See solution cross-references for configuration detail.	solution - http://www.ssh.com/support/documentation/online/ssh/winadminguide/32/Encryption.html solution - http://www.openbsd.org/cgi-bin/man.cgi?query=sshd_config&sektion=5	

10..*.6**	Microsoft FTP Service LIST -R Stack Consumption Denial of Service Vulnerability	21	**Medio**	Stack consumption vulnerability in the FTP server in Microsoft Internet Information Server (IIS) 5.0 and 6.0 allows remote authenticated users to cause a denial of service (crash) via a list (ls) -R command containing a wildcard that references a subdirectory, followed by a .. (dot dot).	This vulnerability was identified because (1) the version of Microsoft FTP Server, 6.0, is less than or equal to 7.5. Paths: /	Upgrade to the latest version of Microsoft IIS.	solution - http://www.microsoft.com/technet/security/Bulletin/MS09-053.mspx solution - http://www.microsoft.com/technet/security/advisory/975191.mspx	CVE-2009-2521
10..**.**1**	Microsoft Active Directory Logon Hours Username Enumeration Weakness	445	Bajo	Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Apply the latest patches for Microsoft Windows	url - http://www.microsoft.com/ solution - http://www.notsosecure.com/folder2/2007/05/27/logon-time-restrictions-in-a-domain-in-windows-server-2003-allows-username-enumeration/	CVE-2007-2999

10..**.10**	Microsoft Active Directory Logon Hours Username Enumeration Weakness	445	Bajo	Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Apply the latest patches for Microsoft Windows	url - http://www.microsoft.com/solution - http://www.notsosecure.com/folder2/2007/05/27/logon-time-restrictions-in-a-domain-in-windows-server-2003-allows-username-enumeration/	CVE-2007-2999
10..**.11**	Microsoft Active Directory Logon Hours Username Enumeration Weakness	445	Bajo	Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Apply the latest patches for Microsoft Windows	url - http://www.microsoft.com/ solution - http://www.notsosecure.com/folder2/2007/05/27/logon-time-restrictions-in-a-domain-in-windows-server-2003-allows-username-enumeration/	CVE-2007-2999

10..**.12**	Microsoft Active Directory Logon Hours Username Enumeration Weakness	445	Bajo	Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Apply the latest patches for Microsoft Windows	url - http://www.microsoft.com/ solution - http://www.notsosecure.com/folder2/2007/05/27/logon-time-restrictions-in-a-domain-in-windows-server-2003-allows-username-enumeration/	CVE-2007-2999
10..**.13**	Microsoft Active Directory Logon Hours Username Enumeration Weakness	445	Bajo	Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Apply the latest patches for Microsoft Windows	url - http://www.microsoft.com/ solution - http://www.notsosecure.com/folder2/2007/05/27/logon-time-restrictions-in-a-domain-in-windows-server-2003-allows-username-enumeration/	CVE-2007-2999

10..**.19**	Microsoft Active Directory Logon Hours Username Enumeration Weakness	445	Bajo	Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Apply the latest patches for Microsoft Windows	url - http://www.microsoft.com/ solution - http://www.notsosecure.com/folder2/2007/05/27/logon-time-restrictions-in-a-domain-in-windows-server-2003-allows-username-enumeration/	CVE-2007-2999
10..**.20**	Microsoft Active Directory Logon Hours Username Enumeration Weakness	445	Bajo	Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Apply the latest patches for Microsoft Windows	url - http://www.microsoft.com/ solution - http://www.notsosecure.com/folder2/2007/05/27/logon-time-restrictions-in-a-domain-in-windows-server-2003-allows-username-enumeration/	CVE-2007-2999

10..**.21**	Microsoft Active Directory Logon Hours Username Enumeration Weakness	445	Bajo	Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Apply the latest patches for Microsoft Windows	url - http://www.microsoft.com/solution - http://www.notsosecure.com/folder2/2007/05/27/logon-time-restrictions-in-a-domain-in-windows-server-2003-allows-username-enumeration/	CVE-2007-2999
10..**.22**	Microsoft Active Directory Logon Hours Username Enumeration Weakness	445	Bajo	Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Apply the latest patches for Microsoft Windows	url - http://www.microsoft.com/ solution - http://www.notsosecure.com/folder2/2007/05/27/logon-time-restrictions-in-a-domain-in-windows-server-2003-allows-username-enumeration/	CVE-2007-2999

10..**.23**	Microsoft Active Directory Logon Hours Username Enumeration Weakness	445	Bajo	Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Apply the latest patches for Microsoft Windows	url - http://www.microsoft.com/ solution - http://www.notsosecure.com/folder2/2007/05/27/logon-time-restrictions-in-a-domain-in-windows-server-2003-allows-username-enumeration/	CVE-2007-2999
10..*.2**	Microsoft Active Directory Logon Hours Username Enumeration Weakness	445	Bajo	Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Apply the latest patches for Microsoft Windows	url - http://www.microsoft.com/ solution - http://www.notsosecure.com/folder2/2007/05/27/logon-time-restrictions-in-a-domain-in-windows-server-2003-allows-username-enumeration/	CVE-2007-2999

10..*.4**	Microsoft Active Directory Logon Hours Username Enumeration Weakness	445	Bajo	Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Apply the latest patches for Microsoft Windows	url - http://www.microsoft.com/ solution - http://www.notsosecure.com/folder2/2007/05/27/logon-time-restrictions-in-a-domain-in-windows-server-2003-allows-username-enumeration/	CVE-2007-2999
10..*.5**	Microsoft Active Directory Logon Hours Username Enumeration Weakness	445	Bajo	Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Apply the latest patches for Microsoft Windows	url - http://www.microsoft.com/ solution - http://www.notsosecure.com/folder2/2007/05/27/logon-time-restrictions-in-a-domain-in-windows-server-2003-allows-username-enumeration/	CVE-2007-2999

10..*.1**	Microsoft Active Directory Logon Hours Username Enumeration Weakness	445	Bajo	Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.	This vulnerability was identified because (1) the version of Microsoft Windows is 5.2 sp2.	Apply the latest patches for Microsoft Windows	url - http://www.microsoft.com/solution - http://www.notsosecure.com/folder2/2007/05/27/logon-time-restrictions-in-a-domain-in-windows-server-2003-allows-username-enumeration/	CVE-2007-2999

Host	Puerto / Servicio	Host	Puerto / Servicio	Host	Puerto / Servicio
10..**.*1**	80/TCP - http	10.**.*.2	10000/TCP - ndmp	10.**.**.13	53/UDP - dns
10..**.*1**	3389/TCP - rdp	10.**.*.2	27000/TCP	10.**.**.13	53/TCP - dns
10..**.*1**	9000/TCP - http	10.**.**.15	3389/TCP - rdp	10.**.**.13	88/TCP - kerberos
10..**.*1**	9001/TCP - http	10.**.*.1	80/TCP - http	10.**.**.13	135/TCP - emap
10..**.*2**	25/TCP - smtp	10.**.*.1	135/TCP - emap	10.**.**.13	137/UDP - netbios-ns
10..**.*2**	80/TCP - http	10.**.*.1	137/UDP - netbios-ns	10.**.**.13	139/TCP - netbios-ssn
10..**.*2**	3389/TCP - rdp	10.**.*.1	139/TCP - netbios-ssn	10.**.**.13	389/TCP - ldap
10..**.*8**	80/TCP - http	10.**.*.1	445/TCP - netbios-ssn	10.**.**.13	445/TCP - netbios-ssn
10..**.*8**	1433/TCP - ms-sql-s	10.**.*.1	1025/TCP - emap	10.**.**.13	464/TCP - kpasswd
10..**.*8**	3389/TCP - rdp	10.**.*.1	1044/TCP	10.**.**.13	593/TCP - emap
10..**.*9**	80/TCP - http	10.**.*.1	1311/TCP - http	10.**.**.13	636/TCP - ldaps
10..**.*9**	3389/TCP - rdp	10.**.*.1	3389/TCP - rdp	10.**.**.13	1026/TCP - emap
10..**.10**	135/TCP - emap	10.**.*.1	4899/TCP - radmin-port	10.**.**.13	1027/TCP - emap

10..**.10**	137/UDP - netbios-ns	10.**.*.1	8000/TCP - irdmi	10.**.**.13	1034/TCP - emap
10..**.10**	139/TCP - netbios-ssn	10.**.*.3	22/TCP - ssh	10.**.**.13	1236/TCP - emap
10..**.10**	445/TCP - netbios-ssn	10.**.*.3	23/TCP - telnet	10.**.**.13	3268/TCP - msft-gc
10..**.10**	1025/TCP - emap	10.**.*.3	80/TCP - http	10.**.**.13	3269/TCP - msft-gc-ssl
10..**.10**	3389/TCP - rdp	10.**.*.3	111/UDP - rpcbind	10.**.**.13	3389/TCP - rdp
10..**.10**	5555/TCP - personal-agent	10.**.*.3	111/TCP - rpcbind	10.**.**.13	5555/TCP - personal-agent
10..**.10**	8000/TCP - http	10.**.*.3	139/TCP - netbios-ssn	10.**.**.19	53/UDP - dns
10..**.10**	9000/TCP - http	10.**.*.3	3144/TCP - **********	10.**.**.19	53/TCP - dns
10..**.11**	21/TCP - ftp	10.**.*.3	5001/TCP - commplex-link	10.**.**.19	135/TCP - emap
10..**.11**	80/TCP - http	10.**.*.3	5307/TCP - sco-aip	10.**.**.19	137/UDP - netbios-ns
10..**.11**	135/TCP - emap	10.**.*.3	5427/TCP - http	10.**.**.19	139/TCP - netbios-ssn
10..**.11**	137/UDP - netbios-ns	10.**.*.3	32768/UDP - filenet-tms	10.**.**.19	389/TCP - ldap
10..**.11**	139/TCP - netbios-ssn	10.**.*.3	32769/TCP - filenet-rpc	10.**.**.19	445/TCP - netbios-ssn
10..**.11**	445/TCP - netbios-ssn	10.**.*.6	21/TCP - ftp	10.**.**.19	464/TCP - kpasswd
10..**.11**	1038/TCP - emap	10.**.*.6	22/TCP - ssh	10.**.**.19	593/TCP - emap
10..**.11**	1052/TCP - emap	10.**.*.6	80/TCP - http	10.**.**.19	636/TCP - ldaps
10..**.11**	1082/TCP - emap	10.**.*.6	3389/TCP - rdp	10.**.**.19	1026/TCP - emap
10..**.11**	1096/TCP - emap	10.**.*.6	5631/TCP - pcanywheredata	10.**.**.19	1027/TCP - emap
10..**.11**	1434/UDP - ms-sql-m	10.**.*.6	8002/TCP - teradataordbms	10.**.**.19	1034/TCP - emap
10..**.11**	1801/TCP - msmq	10.**.*.5	25/TCP - smtp	10.**.**.19	1222/TCP - emap
10..**.11**	1947/TCP - http	10.**.*.5	80/TCP - http	10.**.**.19	3268/TCP - msft-gc
10..**.11**	2103/TCP - emap	10.**.*.5	110/TCP - pop3	10.**.**.19	3269/TCP - msft-gc-ssl
10..**.11**	2105/TCP - emap	10.**.*.5	135/TCP - emap	10.**.**.19	3389/TCP - rdp
10..**.11**	2107/TCP - emap	10.**.*.5	137/UDP - netbios-ns	10.**.**.19	5555/TCP - personal-agent
10..**.11**	3389/TCP - rdp	10.**.*.5	139/TCP - netbios-ssn	10.**.**.20	135/TCP - emap
10..**.11**	5555/TCP - personal-	10.**.*.5	443/TCP - http	10.**.**.20	137/UDP - netbios-ns

	agent				
10..**.12**	135/TCP - emap	10.**.*.5	445/TCP - netbios-ssn	10.**.**.20	139/TCP - netbios-ssn
10..**.12**	137/UDP - netbios-ns	10.**.*.5	587/TCP - smtp	10.**.**.20	445/TCP - netbios-ssn
10..**.12**	139/TCP - netbios-ssn	10.**.*.5	593/TCP - emap	10.**.**.20	1028/TCP - emap
10..**.12**	445/TCP - netbios-ssn	10.**.*.5	995/TCP - pop3	10.**.**.20	1059/TCP - nimreg
10..**.12**	1033/TCP - emap	10.**.*.5	1062/TCP - emap	10.**.**.20	1062/TCP - veracity
10..**.12**	1947/TCP - http	10.**.*.5	1086/TCP - emap	10.**.**.20	1079/TCP - asprovatalk
10..**.12**	3389/TCP - rdp	10.**.*.5	1094/TCP - emap	10.**.**.20	1081/TCP - pvuniwien
10..**.12**	3579/TCP - ttat3lb	10.**.*.5	1095/TCP - emap	10.**.**.20	1089/TCP - ff-annunc
10..**.12**	5555/TCP - personal-agent	10.**.*.5	1132/TCP - emap	10.**.**.20	1092/TCP - obrpd
10..**.**1**	135/TCP - emap	10.**.*.5	1139/TCP - emap	10.**.**.20	1097/TCP - sunclustermgr
10..**.**1**	137/UDP - netbios-ns	10.**.*.5	1171/TCP - emap	10.**.**.20	1149/TCP - bvtsonar
10..**.**1**	139/TCP - netbios-ssn	10.**.*.5	1189/TCP - emap	10.**.**.20	1152/TCP - winpoplanmess
10..**.**1**	445/TCP - netbios-ssn	10.**.*.5	1211/TCP - emap	10.**.**.20	1155/TCP - nfa
10..**.**1**	1026/TCP - emap	10.**.*.5	1272/TCP - emap	10.**.**.20	1158/TCP - dbcontrol-oms
10..**.**1**	1027/TCP - emap	10.**.*.5	3389/TCP - rdp	10.**.**.20	1164/TCP - qsm-proxy
10..**.**1**	3389/TCP - rdp	10.**.*.5	4899/TCP - radmin-port	10.**.**.20	1168/TCP - vchat
10..**.**1**	5555/TCP - personal-agent	10.**.*.5	10000/TCP - ndmp	10.**.**.20	1172/TCP - dnap
10..**.**2**	80/TCP - http	10.**.**.22	445/TCP - netbios-ssn	10.**.**.20	1176/TCP - indigo-server
10..**.**2**	135/TCP - emap	10.**.**.22	1025/TCP - emap	10.**.**.20	1180/TCP - mc-client
10..**.**2**	443/TCP - https	10.**.**.22	1046/TCP - emap	10.**.**.20	1189/TCP - unet
10..**.**2**	445/TCP - netbios-ssn	10.**.**.22	3389/TCP - rdp	10.**.**.20	1194/TCP - openvpn
10..**.**2**	3389/TCP - ms-wbt-server	10.**.**.22	5555/TCP - personal-agent	10.**.**.20	1433/TCP - ms-sql-s
10..**.**2**	5555/TCP - personal-agent	10.**.**.23	80/TCP - http	10.**.**.20	1434/UDP - ms-sql-m
10..**.**2**	49152/TCP - dce	10.**.**.23	135/TCP - emap	10.**.**.20	1566/TCP - corelvideo

10..**.**2**	49153/TCP - dce	10.**.**.23	137/UDP - netbios-ns	10.**.**.20	3306/TCP - mysql
10..**.**2**	49154/TCP - emap	10.**.**.23	139/TCP - netbios-ssn	10.**.**.20	3389/TCP - rdp
10..**.**2**	55220/TCP - dce	10.**.**.23	445/TCP - netbios-ssn	10.**.**.20	3463/TCP - edm-adm-notify
10..**.**2**	62416/TCP - dce	10.**.**.23	1025/TCP - emap	10.**.**.20	5555/TCP - personal-agent
10..**.24**	25/TCP - smtp	10.**.**.23	2383/TCP - ms-olap4	10.**.**.20	6400/TCP
10..**.24**	80/TCP - http	10.**.**.23	3389/TCP - rdp	10.**.**.28	None
10..**.24**	3389/TCP - rdp	10.**.**.23	5555/TCP - personal-agent	10.**.**.21	53/UDP - dns
10..**.29**	None	10.**.*.4	53/UDP - dns	10.**.**.21	53/TCP - dns
10..**.25**	7/UDP - echo	10.**.*.4	53/TCP - dns	10.**.**.21	80/TCP - http
10..**.25**	7/TCP - echo	10.**.*.4	80/TCP - http	10.**.**.21	135/TCP - emap
10..**.25**	22/TCP - ssh	10.**.*.4	88/TCP - kerberos	10.**.**.21	137/UDP - netbios-ns
10..**.25**	80/TCP - http	10.**.*.4	135/TCP - emap	10.**.**.21	139/TCP - netbios-ssn
10..**.26**	7/UDP - echo	10.**.*.4	137/UDP - netbios-ns	10.**.**.21	445/TCP - netbios-ssn
10..**.26**	7/TCP - echo	10.**.*.4	139/TCP - netbios-ssn	10.**.**.21	1025/TCP - emap
10..**.26**	22/TCP - ssh	10.**.*.4	389/TCP - ldap	10.**.**.21	1041/TCP - emap
10..**.26**	80/TCP - http	10.**.*.4	445/TCP - netbios-ssn	10.**.**.21	1077/TCP - imgames
10..**.26**	443/TCP - http	10.**.*.4	464/TCP - kpasswd	10.**.**.21	1079/TCP - asprovatalk
10..*.2**	80/TCP - http	10.**.*.4	500/UDP - isakmp	10.**.**.21	1433/TCP - ms-sql-s
10..*.2**	135/TCP - emap	10.**.*.4	593/TCP - emap	10.**.**.21	1434/UDP - ms-sql-m
10..*.2**	137/UDP - netbios-ns	10.**.*.4	636/TCP - ldap	10.**.**.21	2302/TCP - binderysupport
10..*.2**	139/TCP - netbios-ssn	10.**.*.4	1025/TCP - emap	10.**.**.21	3389/TCP - rdp
10..*.2**	371/TCP - clearcase	10.**.*.4	1027/TCP - emap	10.**.**.21	4899/TCP - radmin-port
10..*.2**	445/TCP - netbios-ssn	10.**.*.4	1039/TCP - emap	10.**.**.21	5555/TCP - personal-agent
10..*.2**	1030/TCP - emap	10.**.*.4	1056/TCP - emap	10.**.**.21	8443/TCP - http
10..*.2**	1038/TCP - mtqp	10.**.*.4	1227/TCP - emap	10.**.**.21	9090/TCP - http
10..*.2**	1046/TCP - wfremotertm	10.**.*.4	1723/TCP - pptp	10.**.**.22	135/TCP - emap

10..*.2**	1050/TCP - emap	10.**.*.4	3268/TCP - msft-gc	10.**.**.22	137/UDP - netbios-ns
10..*.2**	1433/TCP - ms-sql-s	10.**.*.4	3269/TCP - msft-gc-ssl	10.**.**.22	139/TCP - netbios-ssn
10..*.2**	1434/UDP - ms-sql-m	10.**.*.4	3389/TCP - rdp	10.**.**.18	None
10..*.2**	3389/TCP - rdp	10.**.*.4	10000/TCP - ndmp	10.**.**.27	None
10..*.2**	4899/TCP - radmin-port	10.**.**.*3	139/TCP - netbios-ssn	10.**.**.**3	None
10..*.2**	5003/TCP - fmpro-internal	10.**.**.*3	445/TCP - netbios-ssn	10.**.**.*4	None
10..*.2**	8081/TCP - http	10.**.**.14	None	10.**.**.*5	None
10..*.2**	8098/TCP - http	10.**.**.16	None	10.**.**.*6	None
10..*.2**	8099/TCP - http	10.**.**.17	None	10.**.**.*7	None

CONCLUSIÓN

Hay que saber y tener presente que todos y cada uno de los entornos en TI tienen problemas en su estructura, servicios, aplicaciones, configuración, red, etc. y esto conlleva a innumerables vulnerabilidades que pueden ser explotadas y llegar a afectar los planes estratégicos de la organización. El principal efecto perjudicial para una organización que no implante y mantenga correctamente su SGSI es el aumento importante de riesgos, los cuales se convierten en problemas, no sólo aquellos referidos a la seguridad de la información, sino que también afecta a la consecución de objetivos establecidos, a la toma de decisiones y a la posición competitiva en el mercado.

Algunos de los errores por no contar ni implantar y no mantener de un SGSI:

- En cuento a la planificación del proceso de implantación, la escasa adaptación a los objetivos corporativos es bastante común, de hecho, habitualmente se cae en el error de diseñar un SGSI por encima de las necesidades y posibilidades de la organización, por eso es de suma importancia saber que se tiene, con que se cuenta y hasta donde está dispuesta la organización en invertir en este sistema.
- La dependencia absoluta del sistema a una consultora externa. Este error es más común de lo que en un principio pueda parecer y sin ninguna duda es uno de los que más aumenta la probabilidad de fracaso del SGSI.
- Para que la organización cuente con un SGSI óptimo, este debe integrarse perfectamente en las actividades habituales de la organización, de modo que todos los miembros de la institución utilicen e interactúen con el mismo.
- También ocurre todo lo contrario, es decir, la organización es la encargada de todo el proceso. Esto hace que las evaluaciones y controles internos que se llevan a cabo sean, en muchos caos, insuficientes.
- La implantación y el mantenimiento de un SGSI no sólo concierne al departamento relacionado con las TIC, todos y cada uno de los empleados tiene que ser consciente de que papel poseen dentro del sistema, ya que es probable que deban modificar, perfeccionar o rediseñar algunas de sus funciones.
- Lo que hace que un SGSI sea válido y útil es su mantenimiento constante y continuo en el tiempo.