Estudio de recomendaciones sobre Ciberseguridad

Introducción

La seguridad informática busca garantizar la consistencia, integridad y confiabilidad de la información que se gestione a través de medios tecnológicos.

Se parte de la premisa de que no existe la seguridad informática al 100%. Bajo esta óptica, podemos dividir los esfuerzos en esta materia en dos tipos: los que van orientados a mantener la continuidad de los servicios y los que van orientados a recuperarse en el caso en que, a pesar de todos los esfuerzos realizados, se haya presentado una interrupción en los servicios.

El gasto en seguridad informática tiene un comportamiento asintótico con respecto a la mejora que se obtiene al incrementar la inversión en tecnología. Al principio se pueden realizar mejoras muy importantes con poca inversión, pero conforme se avanza las mejoras que se obtienen son cada vez menores y para obtenerlas se requiere un mayor gasto.

Por más esfuerzo que se haga, aún la organización con mayor capital y mayores recursos tendrá aspectos susceptibles de mejora. El límite del gasto que se realiza en esta materia se define con base en una valoración costo – beneficio y en una adecuada administración de riesgos.

El aprovechamiento de los recursos se vuelve por tanto un factor crítico. Sin embargo en la actualidad es posible que los países miembros de cumbre efectúen las mismas pruebas y hasta cometan los mismos errores porque no están compartiendo información.

Se propone la creación de una red de cooperación en materia de ciberseguridad entre los países miembros de la Cumbre Judicial Iberoamericana. La finalidad de esta red es crear un medio para que los especialistas en la materia de los diferentes países puedan compartir las mejores prácticas generando así una sinergia que evite, en la medida de lo posible, el desgaste de esfuerzos y que facilite la cooperación entre los miembros, y la socialización de experiencias con el fin de uniformar la fortaleza ante las amenazas cibernéticas.

Existen diferentes factores que forman parte de los esfuerzos que las organizaciones deben realizar para garantizar la continuidad de los servicios. En el Anexo #1 se listarán estos servicios con la finalidad de que sean considerados sin embargo no serán tratados en la red de cooperación propuesta.

Se presentará a continuación una breve descripción de los aspectos que serán tema de discusión de la red de cooperación. Este listado será socializado con los países miembros para incorporar sus aportes.

La siguiente etapa del proceso será la realización de un diagnóstico, mediante un instrumento idóneo, que permita a cada país determinar los aspectos susceptibles de mejora y los países que podrían colaborar en el proceso.

Recursos específicos para repeler ataques cibernéticos

Los siguientes aspectos serán de interés y discusión en la red de cooperación.

Cultura organizacional

El primer elemento de un esquema de seguridad informática es la cultura de los usuarios. Ningún esquema de seguridad, por más fuerte que sea puede compensar los descuidos y faltas que puedan tener los usuarios. Si los usuarios insisten en abrir correos maliciosos, ingresar a sitios dudosos o utilizar software ilegal, no hay forma de cerrar todos los portillos existentes por lo que mediante estas acciones pondrán en riesgo la seguridad informática de la organización.

Se requiere por tanto que se defina en primera instancia un marco de control, compuesto por políticas, procedimientos, reglamentos y sanciones apoyados y aprobados por la administración superior de la organización.

Pero además se requiere instruir al usuario en temas de seguridad informática de tal forma que tenga los elementos para valorar los riesgos a que se enfrenta y las posibles consecuencias de sus actos. Esto puede realizarse mediante diferentes formas tales como campañas de información sobre diferentes temas y cursos específicos.

Sin temor a equivocarse los esfuerzos que se realicen en estos temas cubren más del 50% del trabajo que implica la seguridad informática de la organización y la inversión requerida para su implementación es relativamente baja.

Elementos del esquema de seguridad informática

Además de la seguridad que se puede implementar propiamente con los componentes de la plataforma tecnológica de la institución (ver Anexo #1) existen una serie de recursos que se adicionan específicamente para solventar debilidades en materia de seguridad informática. Algunos de estos recursos resultan onerosos para muchas organizaciones sin embargo debe valorarse su uso, aún y cuando se limite a áreas muy críticas de la plataforma. También deben considerarse opciones de software libre. Entre estos recursos se puede mencionar:

- Firewall: Estos dispositivos, también conocidos como paredes de fuego, trabajan por denegación por omisión, es decir, lo que no está expresamente autorizado está denegado. Se utilizan para controlar el flujo de información entre dos redes o segmentos de estas. Existen firewalls que trabajan en capas 3 y 4 y otros que trabajan a nivel de aplicación en la capa 7 del modelo OSI. La gama de opciones para un dispositivo de este tipo va desde uno hecho con una PC con dos o más tarjetas de red y una distribución de Linux hasta los más sofisticados que reconocen mediante inteligencia artificial posibles ataques y los repelen. Algunos tienen, previo contrato de servicio, conexión con el fabricante para que este alimente y actualice las firmas (patrones de ataques que reconoce el dispositivo) y las diferentes listas de sitios potencialmente peligrosos para que el administrador defina si se bloquea o se permite el acceso a esos sitios. El fin último de un firewall es permitir el tráfico estrictamente necesario y su efectividad estará en relación directa con la habilidad de su administrador.

- Antimalware: Los delincuentes informáticos generan software que, una vez que ha ingresado en la organización, puede ejecutar diferentes acciones, desde borrar información hasta dar acceso al hacker para que tome control del equipo en que se instaló. Para evitar este riesgo existen productos que se encargan de revisar en cada equipo de la plataforma el software que ingresa. Para que este esquema sea efectivo el software debe estarse actualizando constantemente para incorporar las nuevas amenazas que van surgiendo y para incorporar mejoras a su funcionamiento y efectividad. Estos productos consumen un porcentaje importante de la capacidad de cómputo de los equipos y también tienen un consumo significativo de ancho de banda en la red por lo que su correcta administración resulta crucial para que se constituyan en una solución y no en un problema.
- Antispam: Mención aparte merece el recurso que se encarga de evitar que ingrese correo basura a la organización. Este correo es molesto, consume recursos de red, de almacenamiento y de procesamiento y podrían presentar patrones virales que lo faculten a reproducirse con lo cual se agravan los problemas indicados y además se compromete la credibilidad de la organización al convertirla en fuente de correos indeseados. Sirven además como transporte de otras formas de malware lo que los hace doblemente peligrosos.
- Análisis de vulnerabilidades: Los diferentes productos de software que se instalan en los equipos que componen la plataforma de la organización no son perfectos. Con el paso del tiempo se detectan fallos que los delincuentes informáticos pueden utilizar para sobrepasar los mecanismos de seguridad que se hayan establecido. Estos fallos se conocen como vulnerabilidades. Encontrar y reparar estas vulnerabilidades es una labor titánica por lo que se han desarrollado productos que buscan, con base en la información que publican los distintos fabricantes, estas vulnerabilidades y las informan a tiempo junto con una recomendación para su reparación de tal forma que se hace posible mantener el nivel de vulnerabilidad de los equipos en un rango aceptable. Estos productos deben complementarse con servicios de instalación automatizada de los parches que solventan las deficiencias encontradas.
- Prevención de intrusos: Dado que no se puede asumir que los esquemas de seguridad, en ningún caso, son impenetrables, siempre existe la posibilidad de que un delincuente informático vulnere esas defensas y logre llegar hasta los dispositivos críticos de la organización. Los sistemas de prevención de intrusos contemplan esta posibilidad e incorporan mecanismos para detectar y repeler el acceso de intrusos a los dispositivos clave.
- Administrador de contenidos: A pesar de las advertencias y capacitaciones los usuarios podrían por alguna razón terminar tratando de ingresar a un sitio en internet inadecuado, ya sea por su contenido o porque representa un riesgo potencial para la seguridad informática de la organización. Mediante la administración de contenidos los sitios que se pueden accesar se pueden limitar conforme a las políticas organizaciones evitando riesgos y pérdida de tiempo laboral.
- Correlación de eventos: La mayoría de los dispositivos de la plataforma tecnológica de la organización generan eventos que en forma aislada podrían no dar mayor información pero que si se correlacionan con los que generan otros dispositivos podrían indicar la materialización de algún riesgo. Este tipo de productos buscan recolectar los eventos que generan los distintos dispositivos y realizar una correlación para determinar comportamientos que de otra forma pasarían inadvertidos.

- Auditorías internas y externas en materia de seguridad informática: El esfuerzo por detectar y corregir debilidades debe ser constante. Bajo esta premisa es importante contar con personal especializado a lo interno que realice diferentes estudios e intentos controlados de intrusión con el fin de eliminar los portillos que pudieran utilizar los delincuentes informáticos antes de que estos los encuentren. También se debe contratar, al menos una vez al año, este tipo de revisión por parte de un tercero experto con un enfoque diferente.
- Recursos en línea: Existen numerosos recursos en línea que pueden utilizarse para mejorar la seguridad informática. Tal es el caso del servicio de revisión de páginas web que provee la fundación OWASP (www.owasp.org) o el escaneo de metadatos que ofrece el sitio www.elevenpaths.com mediante su aplicación FOCA. Si bien es cierto no se puede hacer uso de cualquier página, existen servicios como los mencionados que brindan un aporte significativo.
- CSIRT: Dado que no existe garantía de que no se presenten incidentes, la organización debe estar preparada para actuar en estos casos. Un CSIRT es un equipo de respuesta a incidentes, el cual sabe de antemano como se debe actuar en estas situaciones. Este equipo monitorea además las alertas a nivel mundial con la finalidad de prevenir la ocurrencia de incidentes conocidos y mantiene además comunicación con otros equipos similares a nivel mundial con fines de mutua cooperación.

Socialización de los temas de interés

La lista de los temas de interés se va a socializar con todos los países miembros para que sus especialistas puedan hacer aportes. Con la incorporación de los aportes se generará una lista definitiva que se hará de conocimiento de los países miembros.

Se propone el uso de un blog en el que se publicará la lista base que se propone en este documento y se dará un tiempo prudencial para la discusión y definición.

Costa Rica propone hacerse cargo de la implementación de este blog.

Características del instrumento que se definirá

Con base en la lista de los temas que se incluyan como de interés de la red de cooperación se realizará un diagnóstico que permita determinar el nivel de seguridad, de cada país, en cada uno de los aspectos incluidos.

Se propone para este fin la utilización de una encuesta en línea que, en la medida de lo posible, deberá respetar los siguientes parámetros:

- Deberá ser fácil de llenar y tomar el menor tiempo posible
- Deberá respetar la independencia y confidencialidad de los países miembros
- Deberá utilizar una escala que permita la comparación entre los diferentes países

Costa Rica propone hacerse cargo de la implementación de la encuesta en línea.

Análisis de Brecha

El diagnóstico servirá de base para iniciar un proceso de colaboración entre los países miembros en el que, con base en las diferencias encontradas, se definirá la forma en que se minimizará la brecha existente.

Se propone que se definan y prioricen los temas de mayor interés y se busquen mecanismos para compensar las deficiencias. Estos mecanismos van desde la asesoría del país que mayor desarrollo tiene en un tema a los demás hasta la contratación por parte de alguno de los países de un especialista y la posterior replicación del conocimiento y la experiencia a los demás.

Colaboración

Conforme las experiencias positivas y el flujo de información lo permitan, los participantes podrán tener discusiones respecto a las mejoras que se requieren para enfrentar los diferentes retos que presentará el futuro. Se compartirá información respecto al comportamiento de amenazas a nivel mundial y los mecanismos más efectivos para enfrentarlas.

Se espera además que los especialistas puedan realizar investigaciones conjuntas, acordar temas de interés y preparar capacitaciones de unos a otros y que se apoyen cuando alguno tenga un incidente de seguridad que atender.

Mecanismos de integración de la red de cooperación en ciberseguridad

Uno de los principales temas que debe definirse en el proceso de implementación de la red de cooperación es el mecanismo que utilizarán los especialistas para comunicarse en forma efectiva.

Debe ser un medio que permita compartir distintos tipos de información (texto, audio, video) y de preferencia debe tener a los miembros en línea permanentemente.

Se deberá definir también un protocolo para el uso de este medio de comunicación que permita su mejor aprovechamiento.

Conclusiones

El problema de la seguridad informática es común a todos los miembros y todos estamos expuestos a las mismas amenazas por lo que resulta lógico conformar una red de cooperación en materia de ciberseguridad que permita compartir conocimientos y experiencias con que se podrá definir la mejor línea de acción conocida.

Se propone por tanto la conformación de una red de cooperación en materia de ciberseguridad conformada por los especialistas de los países miembros.

Para este fin se propone una lista base de temas que serán considerados de interés para las discusiones de la red de cooperación. Esta lista será socializada mediante un blog que será implementado por Costa Rica. Se dará un tiempo prudencial para recibir aportes. Con base en los aportes de los países miembros se conformará una lista definitiva.

A partir de esta lista se desarrollará una encuesta electrónica que permita el diagnóstico de la situación actual en materia de ciberseguridad de los países miembros.

Este diagnóstico permitirá un análisis de brecha que posibilitará la definición y priorización de los temas que serán abordados inicialmente en la red de cooperación.

La finalidad última de la propuesta es implementar un flujo constante y efectivo de información en materia de ciberseguridad que permita a los especialistas de los países miembros actuar como un solo equipo generando así sinergia.

Para tal fin se requiere de la definición de los mecanismos de comunicación apropiados para este fin y de los correspondientes protocolos para la correcta utilización de estos canales.

Se propone la definición de la lista base definitiva para el siguiente taller preparatorio el cual servirá de base para definir el instrumento de diagnóstico en ese taller. Para este fin se deberá implementar el blog en el mes de junio, permitir la discusión y la incorporación de aportes para el mes de julio. La confección y distribución de la lista definitiva se daría en el mes de agosto.

Anexo #1

Temas que no serán de discusión en la red de cooperación

Marcos de control

En primer lugar es menester indicar que existen múltiples normas, estándares y buenas prácticas que ayudan a ordenar los esfuerzos que se requieren para tener un adecuado control y gobierno de las tecnologías de la información. Es recomendable por tanto aprovechar estos marcos entre los que se pueden citar dos de los más importantes, la familia 27000 de ISO (http://www.iso27000.es/iso27000.html) y el marco de control COBIT en su última versión (http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx).

Seguridad física

Este aparte se refiere a elementos que, sin ser específicamente parte de la plataforma tecnológica, resulta de suma importancia para el funcionamiento de esta. Entre los elementos que se pueden mencionar están:

- Red eléctrica: Los equipos que componen la plataforma tecnológica requieren de energía eléctrica para su funcionamiento. Esta energía debe tener los niveles de calidad establecidos por los fabricantes para que los dispositivos no fallen. Pero además se requiere que el diseño de la red eléctrica soporte los equipos que se van a instalar en cada lugar, se requiere un adecuado sistema de tierras que tal forma que la electricidad sobrante se deseche por los canales apropiados y se requiere que la alimentación eléctrica sea continua lo cual implica la necesidad de contar con sistemas de UPSs y plantas eléctricas que den continuidad al servicio en caso de algún corte en el fluido eléctrico.
- Sistemas de control ambiental: Los equipos informáticos operan en rangos de temperatura y humedad establecidos por los fabricantes. En los lugares donde estas condiciones no se cumplan, ya sea por las condiciones propias de la zona o porque se acumula una cantidad importante de equipos que en conjunto violan estos parámetros, se requiere contar con equipos de control ambiental especializados en equipo electrónico. Nuevamente, la continuidad del funcionamiento de la plataforma tecnológica depende de la continuidad de estos sistemas de control ambiental por lo que se requiere que los diseños garanticen esta operación constante
- Sistemas de vigilancia y alarmas: Existen riesgos que pueden controlarse en forma automática mediante la implementación de sistemas de vigilancia y alarmas en áreas específicas. Entre estos riesgos podemos mencionar los de intrusión, calor, incendio e inundación. También se pueden implementar sistemas de circuito cerrado de televisión con la finalidad de que se pueda ver en forma remota lo que sucede en las áreas sensibles de la plataforma tecnológica.
- Control de Acceso: El acceso a las áreas sensibles, es decir, aquellas áreas donde se ubica equipo clave cuya falla podría provocar discontinuidad en los servicios, debe estar

controlado. Este control puede realizarse en forma manual o electrónica mediante llavines electrónicos y tarjetas codificadas, sin embargo, solo el personal autorizado debe ingresar a estas áreas.

- Extinción de incendio: Un incendio puede provocar daños cuantiosos en muy poco tiempo al equipo electrónico. El fuego debe controlarse en el menor tiempo posible provocando un daño mínimo a los equipos. Los sistemas tradicionales de extinción de incendios resultan inadecuados por lo que debe optarse por un sistema de extinción de incendios especial para equipo electrónico.
- Mantenimiento de todos estos sistemas: Todos los sistemas que garantizan la seguridad física de la plataforma tecnológica requieren de un adecuado mantenimiento. Sin este mantenimiento los sistemas se deteriorarán incrementando el riesgo de falla. Es imprescindible no solo contar con estos sistemas sino que además se debe programar su sostenibilidad.

Refuerzo de la seguridad en los componentes de la plataforma tecnológica

Cada elemento que compone la plataforma tecnológica ofrece posibilidades para incrementar esta seguridad que no se deben desaprovechar. Estas medidas forman parte de los esfuerzos de bajo costo y mucho impacto en el nivel de seguridad informática de la organización. A modo de ejemplo se pueden citar los siguientes elementos y esfuerzos:

- Equipos servidores: los dispositivos en los que se ejecutan los servicios deben estar diseñados para tal fin. Dejando de lado las características de rendimiento que deben exhibir, deben contar con duplicidad en sus componentes críticos (procesadores, fuentes de poder, tarjetas de comunicación, etc., almacenamiento)
- Sistema operativo de los servidores: En primer lugar, el sistema operativo de los servidores controla el acceso a los recursos; como premisa se tiene que nadie debe tener acceso a un recurso que no necesita ni a privilegios de uso que no necesita. Pero además los sistemas operativos permiten la implementación de mecanismos adicionales que refuerzan la seguridad informática como pueden ser mecanismos de replicación de información o incluso servicios. Deben conocerse e implementarse los mecanismos que mayor beneficio aporten.
- Hipervisores: La virtualización permite agregar una capa adicional de seguridad informática ya que facilita mecanismos que permiten incrementar la continuidad de los equipos virtuales y en dado caso reducen el tiempo de su recuperación. Pero además permite una mayor visibilidad en la administración de recursos lo que la faculta para realizar ajustes automáticos a la plataforma que mejoran su desempeño al tiempo que incrementan la continuidad de los servicios. También permiten la implementación de esquemas de intercomunicación de diferentes sitios con lo que se posibilita un mecanismo contingente en caso de una falla de nivel catastrófico de un sitio.
- Dispositivos de almacenamiento: El fin último de la seguridad informática es proteger la información de la organización. No es de sorprender que los dispositivos que almacenan esta información resulten cada vez más sofisticados y confiables, sin embargo, es importante conocer e implementar todas las facilidades que permitan estos equipos. Como ejemplos de estos mecanismos se pueden citar los diferentes arreglos de discos, la duplicidad de componentes y las facilidades para replicación de información.

- Bases de datos: Los motores de bases de datos funcionan como contenedores de la información de tal forma que no se puede acceder a esta sino es a través suyo. Para este fin estos productos implementan mecanismos que refuerzan la seguridad tales como administración de privilegios, filtrado de la información a través de vistas, integridad referencial, encripción tanto en el almacenamiento como en la comunicación, replicación y respaldo de la información. Deben habilitarse tantos mecanismos de seguridad como sea posible.
- Dispositivos de red: Los switches, enrutadores, puntos de acceso y otros dispositivos permiten el acceso a los equipos en los que se almacena la información. Esta función les permite también proveer mecanismos de seguridad que impiden que se utilicen equipos, protocolos o mecanismos para accesar información en forma indebida. Entre estos mecanismos podemos citar las VLANs en los switches, las listas de acceso en switches y enrutadores y hasta el propio diseño de la red en sus diferentes capas.
- Sistemas: Dependiendo de la forma en la que se desarrollen los sistemas informáticos de la organización el código fuente de estos puede constituirse en una debilidad o en una fortaleza. Existen múltiples ataques informáticos que aprovechan descuidos en los programas entre los que se pueden citar la inyección SQL, la ingeniería reversa y las puertas traseras. Es importante que los desarrolladores apliquen buenas prácticas de programación para que sus sistemas formen parte de los muros que protegen la información de la organización. Otro aspecto importante a tener en cuenta es la actualización constante del código; programas desactualizados utilizan componentes desactualizados y potencialmente vulnerables por lo que el código debe estar en constante revisión con el fin de mantenerlo lo más actualizado posible.
- Equipos terminales del usuario: Los equipos terminales son un elemento que comúnmente se descuida y se constituye en punto de falla de la seguridad informática. Debe limitarse lo que el usuario pueda hacer con este de tal forma que un descuido de su parte no comprometa, en la medida de las posibilidades, la seguridad informática de la organización. Deben además deshabilitarse todos los elementos que no deban usarse ya que, en su configuración de fábrica podrían resultar de fácil acceso. También deben habilitarse mecanismos que mejoren la confiabilidad de los equipos, tal es el caso de los discos duros en espejo para evitar pérdidas de información en las computadoras. Es importante aclarar que en este aparte se incluyen también equipos como impresoras que se conectan a la red y que podrían tener habilitados protocolos o servicios que permitan la conexión a la red de un delincuente informático. En este sentido se recomienda estandarizar lo más posible y definir claramente la configuración que cada tipo de dispositivo deba tener.
- Mecanismos de respaldos: El buen uso de estos recursos reduce sustancialmente la pérdida de información. En la actualidad existen múltiples opciones que permiten llevar los tiempos de pérdida de información y de recuperación a valores muy razonables, sin embargo, mientras más eficientes sean estos mecanismos más costosos serán por lo que la organización deberá determinar cuál es el que puede costear y administrar el riesgo residual.
- Sistemas de monitoreo: La mayoría de los componentes críticos de la plataforma tecnológica de una organización son capaces de generar información que permite monitorear su funcionamiento en una o varias consolas lo que permite un manejo preventivo de las fallas o el dado caso una reacción más oportuna ante estas. El monitoreo de la plataforma se convierte por tanto en una herramienta indispensable.