INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY
CAMPUS MONTERREY

PROGRAMA DE GRADUADOS DE LA DIVISIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y ELECTRÓNICA


# "MODELO CORPORATIVO DE MONITOREO DE SEGURIDAD DE INFORMACIÓN A TRAVÉS DE VARIABLES CRÍTICAS OBTENIDAS DE PROCESOS OPERATIVOS DE SEGURIDAD"

**TESIS**

PRESENTADA COMO REQUISITO PARCIAL PARA OBTENER EL GRADO ACADÉMICO DE MAESTRO EN ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

POR:

REY DAVID TAPIA RODRIGUEZ

MONTERREY, N. L. NOVIEMBRE DEL 2005

**Instituto Tecnológico y de Estudios Superiores de Monterrey**
**Campus Monterrey**

**División de Tecnologías de Información y Electrónica**

**Programa de Graduados de la División de Tecnologías de Información y Electrónica**

Los miembros del comité de tesis recomendamos que la presente tesis del Ing. Rey David Tapia Rodríguez sea aceptada como requisito parcial para obtener el grado académico de Maestro en Administración de Tecnologías de Información.

Comité de tesis:

_____

**Ing. Ricardo Morales González,**
**CISA, CISM, BS 7799 Auditor**
Asesor

_____

**Ing. Juan Arturo Nolazco flores, PhD**
Sinodal

_____

**Ing. Ernesto Uriel Rey Guillén,**
**CISSP, CISA, BS-7799 Auditor**
Sinodal

_____

**Ing. David A. Garza Salazar, PhD**
Director del Programa de Graduados en Electrónica,
Computación, Información y Comunicaciones.

**NOVIEMBRE DEL 2005**

# “MODELO CORPORATIVO DE MONITOREO DE SEGURIDAD DE INFORMACIÓN A TRAVÉS DE VARIABLES CRÍTICAS OBTENIDAS DE PROCESOS OPERATIVOS DE SEGURIDAD”


POR:

**Rey David Tapia Rodríguez**


**TESIS**

Presentada al Programa de Graduados de la División de Tecnologías de Información y Electrónica

Este trabajo es requisito parcial para obtener el grado de Maestro en Administración de Tecnologías de Información


**Instituto Tecnológico y de Estudios Superiores de Monterrey**
**Campus Monterrey**


**NOVIEMBRE DEL 2005**

# Dedicatoria

**Hay dos ángeles que durante toda mi vida me han acompañado, que siempre han estado ahí cuando los necesito, que me han dado todo su amor desinteresadamente, que me apoyan aun cuando algunas veces los he decepcionado; pero que no solamente han sido mi apoyo, han sido quienes me han enseñado a valorar la vida y a luchar para salir adelante, quienes me han enseñado a levantarme cuando la vida te hace tropezar, a luchar por los sueños y ha nunca darme por vencido.**

**Hoy les doy gracias por todo lo que han hecho, por que todo lo bueno que como persona puedo tener ellos me lo dieron, y hoy sin duda la culminación de este trabajo ha sido en todos los sentidos gracias a esos dos seres que hasta el día de hoy Dios me permite tenerlos a mi lado.**

**Esas personas son Esteban y Susana a quienes les dedico este trabajo y que además de ser mis ángeles adorados Dios me dio la oportunidad de tenerlos como mis padres.**

**Los amo….**

# Agradecimientos

**A Dios**
Por que me ha dado una vida maravillosa y la oportunidad de culminar hasta el día de hoy los proyectos de vida que me he propuesto.

**A mis hermanas**
Por su cariño y apoyo cuando mas lo he necesitado.

**A mi futura esposa Deniss**
Por tu amor y compresión y por que siempre estas ahí cuando te necesito.

**A mi asesor**
Ing. Ricardo Morales, por su disposición para realizar este proyecto, por la confianza que me demostró y por su apoyo en todo el proceso.

**Al personal de empresa colaboradora**
Ing. Uriel Rey, Ing. Roberto Woo e Ing. Daniel Mijares por su retroalimentación a este trabajo.

**A mis sinodales**
Ing. Arturo Nolazco, Ing. Uriel Rey, por el tiempo que me dedicaron para llevar a buen término este trabajo.

**A mis profesores**
Por compartirme sus conocimientos en el terreno profesional y por sus enseñanzas en el campo personal.

Y a todos los que de alguna manera contribuyeron con este logro. **¡Gracias!**

# Resumen

Existen varios procesos de seguridad como Análisis de riesgos, Administración de procesos del negocio, Concientización de seguridad de información, Política corporativa de seguridad, Control de accesos, equipo de respuesta a incidentes, etc. que han sido desarrollados para garantizar la seguridad de información, pero no existen métricas desarrolladas para monitorear estos procesos y determinar indicadores de seguridad y el estado de estos.

El objetivo de este trabajo fue construir un modelo de monitoreo de seguridad de información a través de variables e indicadores obtenidos de los procesos operativos mencionados anteriormente. Y a través de estas métricas, determinar los niveles de seguridad de información de las empresas que han adoptados estos procesos.

La investigación consistió principalmente en buscar documentos con métricas elaboradas por instituciones reconocidas de clase mundial, que han construido ya métricas de primer nivel, es decir, obtenidas de mejores prácticas.

Además de investigar métricas elaboradas se realizo una investigación profunda de cada uno de los procesos analizando documentos y metodologías encontrados en diferentes fuentes para poder aportar algunas variables adicionales.

Una ves obtenidas estas métricas se trato de determinar la validez de cada una de las variables, Para esto se analizo un caso práctico, que consistió en buscar una empresa para determinar que variables consideraba funcionales y cuales necesitaban modificarse para darles mas sentido a las variables. Las variables que no sean fueron funcionales para la empresa fueron eliminadas.

Adicionalmente se propuso un conjunto de variables e indicadores para monitorear controles comunes derivados del análisis de riesgos, con el fin de darle una perspectiva mas practica al desarrollo de este trabajo.

El resultado fue modelo con diferentes métricas de alto nivel enfocadas a monitorear la funcionalidad de los proceso y de bajo nivel para determinar los niveles de seguridad de en diferentes aspectos que estos contemplan.

INDICE

## Figuras



## Tablas

## Figuras



## Tablas

## Figuras



## Tablas

# Capitulo I.- Introducción

## 1.1.-Situación problemática.

La información es un elemento intangible de las organizaciones, que representa el valor más alto de una organización. Las estrategias que se utilicen en la distribución y el manejo de la información determinaran en que grado se beneficia la empresa. Uno de los aspectos importantes que deben considerarse en el manejo y distribución de información es el control de flujo que debe ejercerse sobre esta. Es importante tener la seguridad de que la información correcta estará con la persona correcta en el proceso correcto y en el tiempo correcto. La mala administración de este proceso de control de flujo desestabiliza la ventaja competitiva de la empresa pues al exponer información importante o confidencial a posibles fugas representa un daño en potencia para las empresas [Espiñeira, Sheldon y Asociados, 2003].

Cuando la era de las computadoras inicio, estas representaron una ventaja para las empresas pues agilizaban procesos internos, mejoraban la calidad de los servicios, y representaban medios de consulta mas rápida. El enfoque que se daba a las computadoras era de contenedores aislados de información que solo ciertas personas podían acceder a través de contraseñas [Bruce Schneir, 2001; Ahmad A Abu-Musa,2004; Doddrell, Gregory R.,1995].

Hoy en día este enfoque ha evolucionado, las computadoras no son solo contenedores aislados de información, la información necesita fluir hacia dentro y hacia fuera de las organizaciones y esto ha llevado a la necesidad de interconectar complejos sistemas de computadoras a través de redes de telecomunicaciones para una mejor circulación de información, desafortunadamente la información no solo pasa a través de las dispositivos también pasa a través de personas, los cuales también son medios de almacenamiento de información. Todo esto hace mas complejo el proceso de control de flujo de información pues la seguridad no solo esta en los dispositivos y equipos electrónicos, si no también en las personas. [M. Farias- Elino, 2003]

A medida que las tecnologías de información se consolidan como una base estratégica para el desarrollo de una empresa. Las amenazas que esto conlleva crecen en forma paralela. Esto debido a que el nuevo modelo de realizar negocios esta cimentado en el uso de las tecnologías de información. Hoy en día el flujo de información de las empresas se realiza a través de distintos medios, equipos y dispositivos tecnológicos, tanto redes de telecomunicaciones como aplicaciones y sistemas de información. La necesidad de estar en comunicación constante con todo el ambiente en el que se desenvuelve la empresa principalmente con sus “stakeholders” tanto externos como internos (inversionistas, administradores, empleados, clientes, proveedores, cadenas de suministro, intermediarios, comunidad y aun con el publico en general)

incrementa las amenazas de perdida de información, entre las amenazas mas importantes que pueden impactar al negocio podemos destacar las que afectan la disponibilidad del flujo de datos (relacionada con la disponibilidad de los servicios), así como las que amenazan la integridad y confidencialidad de la información importante para la empresa.

El no asegurar la disponibilidad integridad y confidencialidad de la información puede llevar a la empresa a enfrentar serios problemas para la continuidad del negocio. En la actualidad existen varios problemas que impiden que estos tres aspectos se cumplan de manera efectiva. Algunos de estos problemas se mencionan a continuación.

- Falta de personal especializado y carencia de referencias internas y externas respecto a las mejores prácticas de seguridad. Esta una característica común en las empresas.

- Falta de una cultura organizacional en el ámbito de seguridad de activos de información, hasta hoy es un factor importante pero no preocupante.

- La Seguridad de Activos de Información en la Compañía es empírica: se carece de presupuesto, herramientas técnicas y adiestramiento del personal administrativo.

- Se conoce de ataques a través del correo externo y de la importancia de tener planes de contingencia, pero no se destina una partida presupuestaria asociado a la Seguridad en TI".

- Se tiene poca perspectiva de visión y poco conocimiento en todos los niveles jerárquicos de la organización sobre la importancia de tener sistemas de seguridad bien definidos.

Cuando se habla de sistemas englobamos todos los elementos que tienen interacción con la información en el contexto de la empresa. Las herramientas que existen hoy en día precisamente buscan definir los métodos más completos que permitan enrobustecer la seguridad en la organización. [Espiñeira, Sheldom y Asociados, 2004]

Los impactos derivados por estos problemas para una empresa se reflejan en perdidas de dinero, productividad, ventaja competitiva, clientes, proveedores, exponen a la empresa a la vergüenza pública y la pueden llevar a la quiebra total.

Cada una de estas pérdidas se puede presentar a través de diferentes factores como son indisponibilidad de los servicios y de las aplicaciones críticas de la empresa. La modificación, corrupción y pérdida de datos que afectan la integridad de la información critica de la empresa. Exponer información

confidencial a terceras personas las cuales pueden hacer uso inadecuado de esta. Utilizándola para un fin perjudicial en contra de la empresa. No podemos tampoco hacer a un lado los daños que pude sufrir la infraestructura del negocio, es decir cualquier evento que cause la destrucción de los dispositivos físicos como los son terremotos, inundaciones, incendios, o cualquier otro evento que este fuera de control humano. Otro factor es la fragilidad de los sistemas de información tanto el hardware como en el software hay una cultura equivocada por parte de la mayoría de los administradores de sistemas y es la de seguridad de producto= funcionalidad 100 %, esto lleva a los administradores a estar confiados en que sus sistemas son seguros y no analizar otras alternativas para el mejoramiento de sus sistemas. Otro factor es la poca cultura de concientización sobre la seguridad de información en las personas. Las personas interactúan y analizan la información de la empresa y estas son también medios de almacenamiento de información. Las personas pueden inconscientemente o concientemente transmitir información a personas no autorizadas [Someswar Kesh, Sam Ramanujan, 2004].

Las organizaciones hoy en día tienen varias inquietudes, esto debido a que cada día observamos en los periódicos, noticieros y otros medios de información ataques de virus, ataques informáticos a las compañías, los cuales ponen a los directivos de las empresas a pensar en soluciones de seguridad.

El aumento en potencia de tecnologías de información cada día mas compleja (WIFI, VoIP, MPLS, PKI, IPSEC, por poner algunos ejemplos) y cuyo uso no podemos hacer a un lado también conllevan a formular planes y modelos de seguridad para el uso eficaz de estas tecnologías.

Existen varias barreras y paradigmas a los que se enfrentan las empresas a la hora de diseñar sus planes de seguridad, por falta de conocimiento e inadecuada implementación de mejores prácticas. Entre estas barreras y paradigmas podemos mencionar los siguientes.

- Inexistencia o ineficiencia de los esquemas de seguridad informática.
- Uso de herramientas tecnológicas sin un previo Análisis de funcionalidad apropiados.
- Creencia de Producto de seguridad = 100% de funcionalidad.
- Compleja interconexión de redes de comunicación, y sistemas de Información.
- Dependencia de las organizaciones en los sistemas de información.
- Falta de cultura y de especialistas en seguridad informática.
- No existe una visión general de la seguridad y su interacción con los demás servicios.
- No existe una figura oficial a quien dirigirse en situaciones de virus, intrusión o robo de información.
- No existe una figura que pueda apoyar en la especificación de un programa general de seguridad.

- ¿Quién registra, responde y da seguimiento a incidentes de seguridad en la institución?
- ¿Quién atiende las demandas de servicios, consultas y soluciones relacionadas a seguridad por parte de los usuarios?
- ¿Qué diferencia hay entre los administradores de servicios de red, DBAs, Webmasters y un encargado de seguridad?

La utilización de software ilegal, el uso indebido del correo electrónico e Internet y la infección por virus informáticos, representan también principales inquietudes de las organizaciones en términos de los eventos de seguridad [computer world, 2004].

Un error común que cometen los administradores de red, es el de no concientizar a los usuarios en la elaboración de sus contraseñas. La mayoría de las personas al manejar varias aplicaciones, tienden a utilizar contraseñas sencillas y fáciles de recordar, no solo en una aplicación, si no que generalmente una vez, seleccionada la contraseña, la utilizan para todas las aplicaciones [Espiñeira, Sheldon y Asociados, 2003].

Otro error común que comenten los usuarios es la administrar en forma poco conveniente el correo electrónico. Por el correo electrónico circula mucha información importante. Y muchas veces esta puede ser enviada por error a personas no autorizas [Parra Alejandro, 2004].

Otro error es la de utilizar cuentas ajenas, esto es un error que trae grandes consecuencias, y generalmente ocurre tanto por parte de administradores como de usuarios [Linda McCarthy (2004)],

Otro error común es el de dejar información importante a las vista, muchas veces los usuarios saben que es hay información o papeles muy importantes, los cuales no deben dejarse a la vista, pero si ellos saben esto, ¿por qué no consideran importante guardar dispositivos de almacenamiento como diskets, CDs, memorias, o cualquier otro tipo de dispositivo que también son importantes? [Robert Durst, Terence Champion, Brian Witten, Eric Miller, Luigi Spagnuolo (1999)].

Se han desarrollo varios procesos y metodologías para mantener la disponibilidad integridad y confidencialidad de la información en una empresa. A continuación se describen algunos de los procesos que podemos encontrar para la seguridad de información de las empresas.

En el **análisis de riesgos** busca determinar la probabilidad de materialización de una amenaza y evaluar el impacto que tendría en el negocio. Este trabajo es complejo dado el volumen de información a recopilar, el conocimiento del riesgo en particular, la dependencia de los criterios a aplicar de acuerdo a la metodología escogida y la adaptación a las necesidades de negocio de la

compañía. Toda circunstancia desconocida involucra necesariamente un elemento probable aleatorio. Cuando se da el caso de que las amenazas se presentan frecuentemente, el elemento aleatorio puede ser modelado bajo un criterio de "frecuencia de aparición", sin embargo, la mayoría de los desastres naturales no ocurren con alta frecuencia. Un análisis de riesgos puede llevarse a cabo en cualquier momento. Tiene como objetivo principal cuantificar las exposiciones existentes con la finalidad de establecer una línea de base para la definición y aplicación posterior de los controles desde el punto de vista del ahorro de costes y balanceo del riesgo [Villalón Antonio,2002 ; Robin L Dillon, M Elisabeth Pate-Cornell, Seth D Guikema, 2003; Computer World, 2004; Bruce Schneier 2001 ].

**BCP** (Bussiness Continuity Plan) que es el **plan de continuidad del negocio** es el que Define las acciones a tomar en los casos en que una determinada contingencia inhabilite algún área de operaciones o tecnología y Permite recuperar las operaciones críticas definidas del negocio.
Este proceso Incluye el DRP (Disaster Recovery Plan) que es el plan de recuperación de desastres. El DRP define las acciones a tomar en los casos en que una determinada contingencia inhabilite el centro de cómputos. Permite recuperar las operaciones críticas definidas de IT [Donald R. Glass,S/F].

**Políticas de seguridad** estas Son creadas de forma explícita para un sistema según su misión, recursos, tipo de red, de usuarios, etc. Contienen los derechos, responsabilidades y sanciones en base a los reglamentos administrativos y técnicos de la institución. Pueden ser un mecanismo de control para definir el buen uso de sus recursos y como apoyo a posteriores procedimientos legales en dado caso. Se dan en cuatro etapas plantación, desarrollo, aprobación, difusión y finalmente su revisión y actualización [Chávez, 2004].

**Concientización** (Awarenness) de la seguridad de información, mediante este proceso se pretende elaborar programas de concientización en las personas sobre la seguridad de información, las personas tienen contacto directo con la información, y muchas veces inconscientemente cometen la indiscreción de transmitirla a terceros, o la hacen llegar a personas que no deben tener acceso a esa información, esto mas que un proceso, es una cultura. Pues generalmente a las personas no se les entrena sobre lo importante que es el manejo y la administración de la información que ellos manejan. Los medios más comunes por los cuales las personas tienden a divulgar inflamación son a través de otras personas, a través del correo, o a través de Internet. Es importante que todas las personas de una empresa participen de igual manera en los procesos o programas de concientizacion desde los mas altos niveles directores ejecutivos y gerentes, hasta los empleados que tiene una funciones muy básicas [Castillo, Di Mare, Díaz, Díez, 2004].

**Respuesta a incidentes** en este proceso debe definirse un plan y una política de manejo de incidentes de seguridad. Los objetivos del plan son: Averiguar

cómo ocurrió el incidente, Averiguar cómo evitar la generación nuevamente del incidente, Determinar el impacto y daño del incidente (limitarlo), Recuperar el sistema del incidente (retomar el control), Actualizar la política de seguridad y sus procedimientos, Averiguar quién provocó el incidente [Georgia Killcrece, 2004].

**Control de acceso** que se refiere a un conjunto completo de procedimientos ejecutados por hardware, software y administradores, para monitorear accesos, identificar usuarios requerientes de accesos, registrar intentos de acceso, y otorgar o denegar accesos de acuerdo a reglas predeterminadas, lo que se busca con este procedimiento es proteger con el Control de Accesos Datos Divulgación, modificación y copiado no autorizado. Sistemas Uso, modificación y denegación de servicios no autorizados. Los tipos de controles de accesos son: Controles Administrativos: Esta categoría incluye Políticas y procedimientos, security awareness, entrenamiento, background checks, estudios de hábitos de trabajo, supervisión, etc. Controles Lógicos y Técnicos: Implica la restricción del acceso a los sistemas y la protección de la información: encriptación, smart cards, ACLs, etc. Controles Físicos: Esta categoría incluye guardias, seguridad física del edificio en general, separación de funciones, back up, etc. Existen además controles que puede ser la combinación de cada uno de ellos [Donald R. Glass, S/F].

El **proceso de monitoreo** es el mas importante de todo, pues este proceso busca definir las métricas e indicadores que ayudarán a determinar los niveles de funcionalidad de los diferentes procesos (Bruce Schneir, 2001).

En todos estos procesos se necesita obtener periódicamente información acerca de su desempeño, con el fin de monitorear la eficiencia y efectividad de su gestión, de manera que permitan tomar decisiones oportunas sobre posibles riesgos que puedan presentarse y validen además la efectividad de los controles establecidos. La manera tradicional para realizar esta labor ha sido mediante indicadores, los cuales representan una medida de la condición de un proceso o evento en un momento determinado, proporcionando un panorama de la situación del mismo. El uso de indicadores debe establecer tanto los procesos operativos como los administrativos en una organización, y derivar acuerdos de desempeño basados en la aplicación y uso correcto de los programas o procesos, en el caso de este documento nos referimos a los procesos de seguridad de información.

Los indicadores constituyen la manera por la cual se retroalimenta un proceso, se monitorea el avance o la ejecución del mismo y se respaldan los planes establecidos, y tienen mayor relevancia, si el tiempo de respuesta es inmediato, o muy corto.

Una de las formas en que se puede llevar a cabo el establecimiento de los indicadores, es a través de los Indicadores Claves de funcionalidad (KPI, por sus siglas en inglés-*key Performance Indicators*).

Cada uno de estos procesos ataca ciertas vulnerabilidades de la empresa con respecto a la seguridad de información. El objetivo principal de cada uno de ellos es la de analizar cada vulnerabilidad y proponer modelos o controles a través de los cuales se pueda contrarrestar cualquier amenaza. Todos ellos siguen un protocolo clave que es: que queremos proteger?, contra quien lo queremos proteger?, cuanto tiempo queremos protegerlo?, y como lo vamos a proteger? La implementación de cada proceso involucra la participación de recursos financieros, recursos materiales y de personas. Aun cuando las empresas implementen ciertos procesos y metodologías, sigue existiendo el riesgo de que estos fallen y las vulnerabilidades continúen. A pesar de esto, es importante que las empresas estén concientes de que la seguridad de la información es importante pues su objetivo es preservar los activos y mantener la operabilidad de la organización, por eso es necesario implementar sistemas de monitoreo de seguridad que realimenten variables clave previamente definidas y que estas nos ayuden a construir métricas para determinar los niveles de seguridad de información de una empresa.

## 1.2.-Problema.

Existen varios procesos operativos que se pueden implementar en seguridad de información, pero son nulas las métricas existentes para el monitoreo de cada proceso, haciendo complicado determinar el estado y grado de eficiencia o funcionalidad de estos.

“Uno los mayores retos para las organizaciones es encontrar y utilizar un modelo efectivo y probado para la seguridad de la información e incorporar este modelo a la Organización”[Espiñeira, Sheldom y Asociados 2004].

Considerando además que un sistema sin retroalimentación se degenera, o lo que es igual si a un sistema se introduce basura a la salida tendremos basura, necesitamos entonces un sistema de retroalimentación que lleve el sistema al estado deseado (Gonzalez, 2004).

De aquí podemos concluir que es necesario un modelo de monitoreo de procesos de seguridad de información que contenga primeramente variables obtenidas de los diferentes procesos, que nos ayuden en la construcción de métricas para determinar el nivel de eficiencia y funcionalidad, así como el estado de estos procesos.

En segundo lugar este modelo debe incluir indicadores, que son las métricas que determinaran el estado y grado de eficiencia de cada uno de los procesos, y

así mismo poder utilizar estas métricas para realizar la retroalimentación necesaria en estos procesos.

El modelo tradicional de seguridad utilizado por las empresas, es el siguiente.

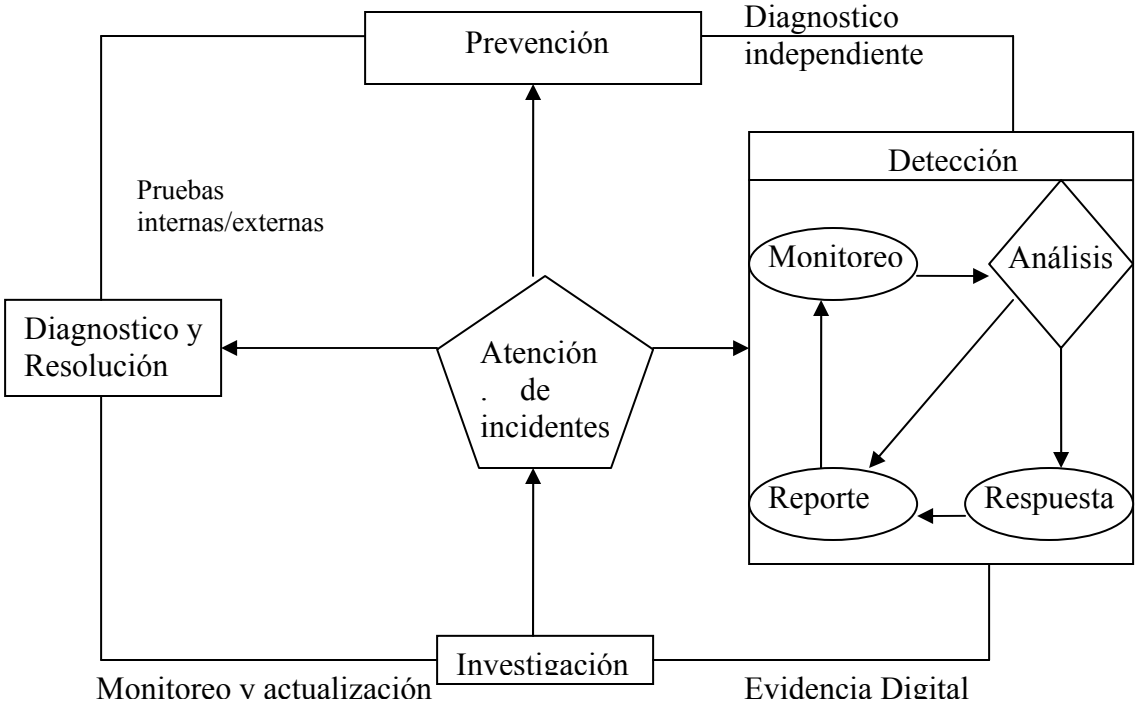



Figura 1.- Modelo de seguridad

En el modelo se pueden encontrar básicamente 4 etapas, la primera etapa es la detección, en esta etapa se analizan los problemas que ocurren en un momento dado, como por ejemplo un posible ataque o cualquier otro incidente de seguridad. Esta primera etapa se subdivide en 4 etapas: el monitoreo consiste en un chequeo constante de los procesos, en el análisis se revisa los problemas que están ocurriendo y después se propone una posible respuesta. En el reporte se documenta todo lo relacionado al incidente de seguridad, con el fin de llevar un control de estos incidentes y poder contar además con un estadístico para determinar que incidentes se repiten constantemente.
En la investigación se realiza un análisis sobre las posibles razones que pudieron influir para que el incidente ocurriera.
En el diagnostico y resolución se resuelve el incidente y se implementa la solución, además se termina de documentar el incidente para poder contar con información para la prevención de futuros sucesos similares.
Y finalmente en la última etapa se utiliza la información obtenida de incidentes anteriores para poder prevenirlos en el futuro.
El problema que podemos observar en este modelo es que no existe una definición clara del proceso de monitoreo, es decir, que podemos monitorear

dentro de los procesos que nos puedan generar los indicadores para determinar los niveles de seguridad y el estado de los procesos.

## 1.3.-Objetivos.

Objetivo 1.- Proponer un modelo de monitoreo bajo un esquema corporativo, que genere Indicadores de la seguridad de información, incorporando las variables de cada Proceso básico de seguridad.

Objetivo 2.- El segundo objetivo consiste en una vez encontradas las variables construir indicadores estableciendo relaciones entre estas variables.

Objetivo 3.- En todo análisis de riesgos existe un conjunto de controles que son necesarios implementar independientemente de la aplicación, el objetivo es determinar métricas para el monitoreo de dichos controles.

# Capitulo 2.- Marco Teórico

## *Marco teórico*

### 2.1.-Tecnologías de la información

Las tecnologías de información son tan necesarias en una organización que han llegado a constituirse una ventaja competitiva para la empresa. Gran parte del desarrollo tecnológico en este sentido se ha dado por la necesidad de las empresas de agilizar sus procesos y modelos de negocios para ser cada día organizaciones más eficientes y productivas.

Hoy en día se habla mucho de la alineación al negocio, de tal manera que la alineación de tecnologías de información al negocio constituye una de las preocupaciones más importantes para las organizaciones.

Las tecnologías de la información se tornan cada día más complejas. La complejidad de estas hace más difícil la administración llevando por tanto a una difícil alineación de tecnologías de información al modelo y plan de negocio.

La correcta administración de los sistemas de información es responsabilidad de todos los niveles jerárquicos de la organización. Tanto los directivos, administradores operativos y usuarios deben tener esa responsabilidad.

Hoy se habla de que hay mas conciencia en los directivos de empresas sobre lo importante que es la seguridad de información en la corporación, sin embargo los recursos financieros y humanos destinados para el desarrollo de planes y procesos de seguridad siguen siendo relativamente bajos(Revista gerencia, 2004).

Los administradores operativos se encargan de la operación y el buen funcionamiento de las tecnologías, los administradores de sistemas por ejemplo se encargan de mantener los sistemas información funcionando, pero tienden a no visualizar la necesidad de de mantener la seguridad en estos sistemas. Esto se debe a que la seguridad no depende solo de ciertos factores meramente tecnológicos sino que involucra factores de toda la organización y pudiendo ser estos internos o externos. Por ejemplo, cuando en una empresa se desarrolla una aplicación para un determinado proceso generalmente los desarrolladores se enfocan a la funcionalidad, pero muy poco o nada al desarrollo de controles de seguridad para esa aplicación.
Aun cuando se puedan desarrollar directivas de seguridad para las tecnologías de información, la poca cultura que tienen los usuarios sobre la protección de

información hace que muchas veces las directivas de seguridad de las tecnologías de información sean vanas. De que sirve tener una caja fuerte con el mapa de un tesoro, si describo a otras personas los mapas del tesoro. De aquí que la falta de políticas y procedimientos de seguridad es uno de los problemas más graves que afrontan las empresas hoy en día en lo que se refiere a la protección de sus activos de información frente a amenazas externas e internas [[John Markoff, John Schwartz, 2002].

## 2.2.-Arquitectura corporativa de seguridad de información.

Durante mucho tiempo la mayoría de las corporaciones, no han considerado importante el desarrollo de planes de seguridad. Sobre todo a nivel gerencia o de dirección. El poco conocimiento sobre el tema de seguridad de información, tanto por los directivos y los administradores de tecnologías de información es la razón principal del por que las corporaciones no destinan recursos humanos y financieros a esta área. Aun cuando la iniciativa de crear planes de seguridad surja por parte de los administradores de tecnologías, al enviar las propuestas sobre seguridad, las evaluaciones de estas por parte de los directivos son tardadas, y casi siempre caen en cajón de propuestas de poca prioridad, por no poder observar en el documento la importancia necesaria.

Antes de realizar la propuesta, se debe realizar un estudio profundo para saber en que puntos la empresa es vulnerable, y toda esta información debe estar explicada en la propuesta. Este estudio generalmente es tardado, pero vale la pena par poder detectar las fallas más importantes aun cuando estas puedan parecer sin importancia o mínimas. Por los directivos pasan miles de documentos, al elaborar una propuesta de proyecto de seguridad esta debe ser clara, concisa y bien redactada. Para que al ser evaluada por los directivos pueda ser de interés y mostrar las ventajas de la propuesta y las consecuencias de no implementarla. Una propuesta mal elaborada en cada uno de sus puntos solo crea en los directivos poca visión del problema y como consecuencia que no vean los beneficios y como consecuencia. También, se invalida la utilidad del análisis de la propuesta [M. Farias- Elinos].

Un problema en las corporaciones es que muchas veces el implementar un plan o proyecto de seguridad no se alcanza todos los niveles jerárquicos de una corporación. Es frecuentemente el nivel gerencia y de dirección el menos protegido y más importante a proteger, pues es en estos niveles donde se encuentra concentrada la información critica de la empresa, como los estados financieros, estrategias del negocio, planes a corto y a largo plazo. Esto se debe a la cultura de que a los jefes no hay que tocarlos. Y muchas veces ellos defienden la invasión a sus pertenencias. Además casi siempre prefieren estar al margen de un proyecto. Caso particular es que al recopilar información para la propuesta siempre es difícil acceder a sus maquinas para saber si tienen las directivas de seguridad apropiadas. Y al implementar los proyectos ellos son el

nivel jerárquico más difícil de atacar por la poca disponibilidad y participación de este nivel [Linda McCarthy (2004)].

Al elaborar una propuesta para una empresa que se inicia en los laureles de la seguridad, esta incluirá seguramente la necesidad de recursos financieros, lo cual levantara una primera barrera entre los directivos y la propuesta. A los directivos les encanta las finanzas, por eso elaborar diagramas de perdida de ingresos por los problemas de amenazas y diagramas de costo beneficio por la implementación de controles de seguridad ayudan mucho a la hora de revisar la propuesta. Estos diagramas despiertan más el interés de los directivos.

Por otro lado seguramente necesitaremos personal para el desarrollo del plan de seguridad. Un paradigma fuertemente arraigado por parte de los directivos es que las tecnologías de información son asunto de sistemas. Así que lo mas seguro es que creerán que la seguridad es asunto de los administradores de sistemas. Es preciso aclarar en la propuesta que la seguridad es un problema corporativo, así que la seguridad es asunto de todos. Un administrador de sistemas puede conocer algunos líneamientos de seguridad pero también es verdad que un administrador de sistemas la mayoría de las veces no conoce el funcionamiento y la estructura de una organización. Es por eso que ser asesorados externamente o el contratar a un experto en seguridad para implementar un plan de seguridad ayudaría bastante. Cada departamento en la organización jugara un papel importante en el plan de seguridad, así que es necesario juntar personal de cada departamento para explicar y presentar el plan de seguridad. Además será necesario establecer nuevas responsabilidades y nuevos roles dentro de la empresa algunos tomados por personal ya existente y algunos otros por nuevos empleados.

Dentro de la estructura del plan de seguridad se puedan crear nuevas posiciones y departamento como por ejemplo las siguientes:

- El administrador de seguridad
- Un equipo de seguridad
- Un comité ejecutivo de seguridad
- Coordinadores de seguridad
- Operadores de aplicaciones

Cada uno tendrá roles definidos pero lo que es importante destacar es que debe existir una comunicación fluida entre cada uno de los elementos para mantener el plan de seguridad funcionando efectivamente.

## 2.3.- Variables e indicadores

Hay variables que pueden ser comunes en la implementación de cada proceso, aun cuando las empresas puedan tener diferentes necesidades. Lo importante es poder determinar, cuales son las variables críticas en cada proceso. Es decir que variable en si, constituyen una base importante de monitoreo de la cual se pueda extraer información impórtate que arroje resultados sobre los sistemas que están siendo vulnerados y poder corregir los problemas a tiempo.

En cada uno de los procesos existen ciertas variables que hay que considerar, los procesos utilizados en si no tienen un Standard en su aplicación, las variables a considerar en cada proceso depende del giro de la empresa, de la tecnología de información que utilice y del tipo de información que busque proteger [Sanderson, Ethan, Forcht, Karen A. (1996)].

Como en cualquiera otra actividad de la organización, el desarrollo de la cultura organizacional necesita obtener periódicamente información acerca de su desempeño, con el fin de monitorear la eficiencia y efectividad de su gestión, de manera que permita tomar decisiones oportunas sobre posibles riesgos que puedan presentarse y la efectividad de los controles establecidos. La manera tradicional para realizar esta labor ha sido mediante indicadores, los cuales representan una medida de la condición de un proceso o evento en un momento determinado, proporcionando un panorama de la situación del mismo. El uso de indicadores debe establecer tanto los procesos operativos como los administrativos en una organización, y derivar acuerdos de desempeño basados en la aplicación y uso correcto de los programas, como en el caso de este documento, de los programas de concientización, entrenamiento, y educación aplicados al interior de la organización.

Los indicadores constituyen la manera por la cual se retroalimenta un proceso, se monitorea el avance o la ejecución del mismo y se respaldan los planes establecidos, y tienen mayor relevancia, si el tiempo de respuesta es inmediato, o muy corto.

La forma como se puede llevar a cabo el establecimiento de los indicadores, es a través de los Indicadores Claves de funcionalidad (KPI, por sus siglas en inglés-*key Performance Indicators*) cuya definición puede tener la siguiente forma:

- Titulo del indicador Clave de desempeño
- Define
- Mide
- Objetivo

El monitoreo de cualquier proceso de negocio pasa por el establecimiento de una serie de indicadores, los Key Performance Indicators (KPI) o Indicadores Clave de Rendimiento, que dan idea del funcionamiento de los procesos críticos de negocio.

En un proceso de negocio con entidad suficiente el número de estos indicadores puede no ser trivial de manejar en formato numérico. Por ello una buena parte de los proveedores de este tipo de tecnología terminan representando gráficamente el conjunto de indicadores en forma de cuadro de mandos o dashboard.

El cálculo de los indicadores clave se suele complementar con un conjunto de reglas que permiten disparar las alarmas cuando alguno de los indicadores muestra una tendencia que puede conducir a un problema potencial. La alarma se puede vehicular incluso por telefonía móvil, con el objetivo de posibilitar la reacción inmediata en procesos críticos.

De nuevo es aquí donde la visualización de información, especialmente de series temporales y de las relaciones entre unos sucesos y otros, nos puede ayudar a identificar patrones de comportamiento de negocio y relaciones de causa-efecto entre grandes cantidades de sucesos que, de otra forma, serían muy difíciles de identificar ( Dürsteler, 2003).

En el seminario del Profesor Mario Vogel, se define una ruta interesante para la definición de indicadores:

**Ruta metodológica para establecer indicadores**

| | |
|---|---|
| **Objetivo** | Declaración de lo que la estrategia debe lograr y qué es crítico para su éxito |
| **Aclarar** | Qué queremos realmente conseguir (Aclarar cual es el objetivo buscado) |
| **Variables que muestren logros** | Hallar las variables críticas del objetivo buscado (FCE)<br>(Cómo nos damos cuenta que lo estamos logrando) |
| **Indicador** | Hallar los indicadores adecuados para cada variable<br>¿Cuáles son los indicadores críticos que indican nuestra dirección estratégica? |

**EJEMPLOS**

| | |
|---|---|
| **Objetivo** | Efectividad Comercial |
| **Aclarar** | Utilizar todos los recursos comerciales para vender más |
| **Variables críticas** | Si la fuerza de Ventas es Eficiente<br>Si la publicidad es recordada y además es útil<br>Si el canal de distribución aumenta su participación |
| **Indicador** | % de Aumento de la rentabilidad<br>Top of mind<br>Numero de nuevos clientes<br>% de aumento de participación en el canal |

| Objetivo | Ser una facultad reconocida regionalmente |
|---|---|
| Aclarar | Mejores oportunidades de trabajo para egresados<br>Captar los mejores talentos de la región<br>Incrementar Ingresos |
| Variables críticas | Egresados con puestos directivos<br>Alumnos con promedios de excelencia<br>Superar punto de equilibro |
| Indicadores | # de egresados con puestos directivos<br># de alumnos con mayor promedio a 9 que ingresan<br>Períodos con excedente financiero |

Tabla 1.- Tipos de indicadores

En ningún momento es conveniente partir de un indicador para definir un objetivo.

Lo correcto es aclarar primero cual es el objetivo buscado. La secuencia lógica e internacionalmente aceptada es: Objetivo, indicador, meta. El proceso de definición de indicadores, requiere que se defina con claridad "qué medir, cómo medir, cuándo medir, fuente de la medición y responsable" (Kaizen, 2004).

## 2.4.- Eventos, amenazas, incidentes, vulnerabilidades y riesgos.

Los eventos que pueden ocurrir en una empresa y que puedan poner en peligro la información son diversos y muy variados, y muchas veces fuera del alcance de los planes de seguridad. Como por ejemplo terremotos, inundaciones, nevadas, huracanes u otros desastres naturales, también es importante considerar los ataques físicos a la infraestructura como pueden ser por manifestaciones, conflictos armados, ataques terroristas o invasiones extranjeras. También es importante considerar los eventos internos, como pueden ser incendios, fallas eléctricas, desconexión no intencional de un equipo o tecnología que almacena información, o daño físico a los equipos por parte de los usuarios [Anónimo (2004)].

Las amenazas son agentes capaces de explotar los fallos de seguridad, que Denominamos puntos débiles y, como consecuencia de ello, causar pérdidas o Daños a los activos de una empresa, afectando a sus negocios (ALSI, 2004).

Los activos están constantemente sometidos a amenazas que pueden colocar en riesgo la integridad, confidencialidad y disponibilidad de la información. Estas amenazas siempre existirán y están relacionadas a causas que representan riesgos, las cuales pueden ser:

Causas naturales o no naturales
Causas internas o externas

Por lo tanto, entendemos que uno de los objetivos de la seguridad de la información es impedir que las amenazas exploten puntos débiles y afecten

alguno de los principios básicos de la seguridad de la información (integridad, disponibilidad, confidencialidad), causando daños al negocio de las empresas.
Dada la importancia de las amenazas y el impacto que puede tener para la información de las organizaciones revisemos ahora su clasificación.

1. Amenazas naturales – condiciones de la naturaleza y la intemperie que podrán causar daños a los activos, tales como fuego, inundación, terremotos.

2. Intencionales – son amenazas deliberadas, fraudes, vandalismo, sabotajes, espionaje, invasiones y ataques, robos y hurtos de información, entre otras.

3. Involuntarias - son amenazas resultantes de acciones inconscientes de usuarios, por virus electrónicos, muchas veces causadas por la falta de conocimiento en el uso de los activos, tales como errores y accidentes.

Un incidente es un evento de riesgo no tan severo, es decir no significa que los sistemas queden completamente fuera de servicio o inhabilitados, son más bien eventos aislados. Estos pueden ser ataques externos como un hacker o cracker tratando de dañar el sistema. Para cada uno de estos incidentes se debe tener un plan de acción que pueda llevarnos a corregir cada uno de estos incidentes, el plan de acción debe contener al menos la siguiente información: en que consiste el incidente, que provoco el incidente y los pasos a seguir para corregirlo y finalmente determinar una acción para que el incidente no vuelva a pasar [SVIS-E business].

Las amenazas siempre han existido y es de esperarse que conforme avance la tecnología también surgirán nuevas formas en las que la información puede llegar a estar expuesta, por tanto es importante conocer el marco general en cómo clasifican las vulnerabilidades o puntos débiles que pueden hacer que esas amenazas impacten nuestro sistemas, comprometiendo los principios de la seguridad de nuestra información.

Los puntos débiles son los elementos que, al ser explotados por amenazas, afectan la confidencialidad, disponibilidad e integridad de la información de un individuo o empresa. Uno de los primeros pasos para la implementación de la seguridad es rastrear y eliminar los puntos débiles de un ambiente de tecnología de la información (ALSI, 2004).

Al ser identificados los puntos débiles, será posible dimensionar los riesgos a los cuales el ambiente está expuesto y definir las medidas de seguridad apropiadas para su corrección.

Los puntos débiles dependen de la forma en que se organizó el ambiente en que se maneja la información. La existencia de puntos débiles está relacionada con

la presencia de elementos que perjudican el uso adecuado de la información y del medio en que la misma se está utilizando.

Podemos comprender ahora otro objetivo de la seguridad de la información: la corrección de puntos débiles existentes en el ambiente en que se usa la información., con el objeto de reducir los riesgos a que está sometida, evitando así la concretización de una amenaza.

Los tipos de amenaza pueden ser: Físicas, naturales, de hardware, de software, de manejo de almacenaje, de comunicación, humanas.

El riesgo es la probabilidad de que las amenazas exploten los puntos débiles, causando pérdidas o daños a los activos e impactos al negocio, es decir, afectando: La confidencialidad, la integridad y la disponibilidad de la información. Concluimos que la seguridad es una práctica orientada hacia la eliminación de las vulnerabilidades para evitar o reducir la posibilidad que las potenciales amenazas se concreten en el ambiente que se quiere proteger. El principal objetivo es garantizar el éxito de la comunicación segura, con información disponible, íntegra y confidencial, a través de medidas de seguridad que puedan tornar factible el negocio de un individuo o empresa con el menor riesgo posible (ALSI, 2004).

## 2.5.- Monitoreo

Monitorear la seguridad de un edificio implica muchas cosas. Implica una serie de sensores alrededor del edificio. Implica además una central de alarmas que se activa si los sensores detectan algo. Esto debe implicar alguna clase de respuesta por parte de la alarma. De que sirve tener una alarma si no se deriva alguna respuesta. Cuando sucede esto la alarma no genera ningún valor.

En una red implica cosas similares. Existe una serie de sensores alrededor de la red. Cada firewall produce una serie de mensajes, al igual que cada router y cada servidor. Un sistema detector de intrusos (IDS) envía un mensaje cuando algo pasa. Y así cada producto genera alarmas cuando algo esta sucediendo.

Pero cada una de estas alarmas activadas por los sensores no ofrecen seguridad por si solas. Estas llegan a ser ineficientes si solo detectan comportamientos los comportamientos extraños y anómalos.

Las alarmas en una casa pueden detectar cosas simples como un vidrio roto, un intruso caminado por un pasillo, etc. El valor de estas alarmas radica en que al activarse puedan notificar a las personas apropiadas para que ellas puedan actuar. Si nosotros aplicamos este mismo principio de monitoreo a red seria mas complicado.

En las redes, el monitoreo es el lazo de retroalimentación que hace mas efectivas las actividades seguras en la red. Es a través del monitoreo como los responsables de seguridad pueden determinar donde instalar dispositivos de seguridad para conseguir resultados efectivos y determinar donde no tendrían un buen funcionamiento. Así como conocer si los dispositivos de seguridad están bien configurados, y poder tener mayor seguridad de donde los sistemas pueden ser atacados.

En la actualidad algunas compañías opinan que el monitoreo es algo que se debe realizar después de haber adquirido productos de seguridad (firewall, IDS, etc.), después de haber desarrollado políticas, después de haber realizado análisis de vulnerabilidades. Esto no tiene mucho sentido.

El monitoreo debe ser el primer paso en un plan de seguridad, y es lo primero que se puede hacer para poder proyectar un plan que pueda generar valor. El monitoreo es la herramienta que te ayudar en el análisis de la política, en la valoración de vulnerabilidades y en la selección de dispositivos tecnológicos de seguridad. El monitoreo asegura que lo que estas aplicando es lo que realmente necesitas (Bruce Schneir, 2001).

## 2.6.- Modelo propuesto para la seguridad de información.

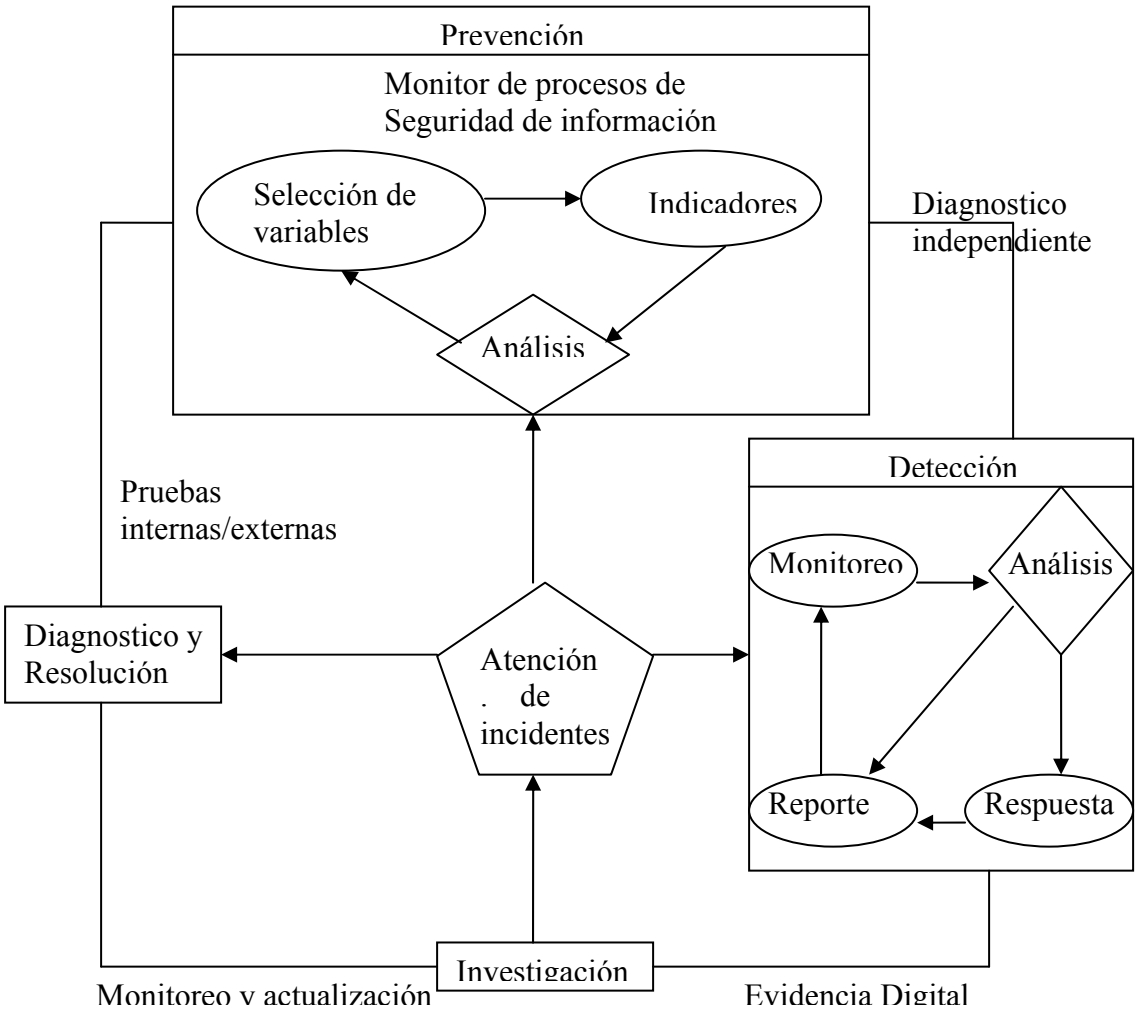



Figura 2.- Modelo de propuesto de seguridad corporativa

## 2.7.-Descripción de modelo propuesto.

En el modelo corporativo tradicional se desarrollan cuatro etapas importantes. En la primera, se lleva a cabo la detección de eventos o incidentes para posteriormente investigar las causas y llevarlos a su corrección. En el modelo propuesto el mayor énfasis se da en prevención de eventos e incidentes monitoreando los procesos de seguridad de información. Con esto, en primer lugar se pretende contar con variables que nos puedan arrojar información sobre los niveles de seguridad y estado de los procesos. Además, se pueden prevenir muchos incidentes antes de que estos ocurran, eliminando en algunos casos la necesidad de investigación, de diagnostico y de resolución.

En la prevención se pude llevar acabo el monitoreo de procesos similar al de la etapa de detección. Este empieza con la selección de variables críticas. Es decir, seleccionar las variables realmente importantes y que arrojen información sobre los eventos o incidentes que estén ocurriendo constantemente o que estén próximos a ocurrir. Después de proponer estas variables se pueden construir indicadores que son las métricas que finalmente nos dan una medición de los niveles de seguridad y estado de los procesos. En el monitoreo se observa el comportamiento de las variables y las métricas, para recolectar información importante y poder analizarla.

En el análisis se determina si la información esta arrojando los resultados esperados. Es decir, determinar si las variables reflejan la información que nos ayudará a monitorear los eventos o incidentes que pondrán en riesgo nuestra información. Este proceso en la prevención debe ser constante, si nuestro proceso de monitoreo falla, entonces seria necesario analizar si en conjunto de variables propuestas son las indicadas.

Otra ventaja que presenta el modelo propuesto es que se pueden detectar pequeños incidentes, que pudieran no representar un peligro potencial para la información en determinado momento. Pero, que de no tomarlos en cuenta, estos incidentes pueden llegar a constituir una amenaza muy peligrosa.

## 2.8.- Metodología de investigación.

**Tipo de estudio.**

El tipo de estudio que se realizara es explicativo, a través de la investigación se determinará el comportamiento de las variables críticas y también a través de un estudio de correlación se estudiara la influencia que ejercen unas sobre otras. Otro aspecto importante que se pretende obtener del estudio será determinar la factibilidad de las variables que se manejen para su integración en nuestro modelo. En el caso de que estas no sean las variables apropiadas, buscar el conjunto de variables mas apropiado que nos arrojen los datos esperados

La población en general que contamos para esta tesis son todas las empresas que utilizan redes de información. Para poder llevar acabo la investigación propuesta y poder analizar los procesos de seguridad (análisis de riesgos, BCP, política corporativa, concientización, control de accesos, análisis de incidentes), nos apoyaremos en una corporación real que ya ha implementado algunos de estos procesos.

**Descripción del estudio.**

En primer lugar se pretende conocer un poco sobre la teoría de los procesos de seguridad de información que existen, como están estructurados, diferentes metodologías de implementación y que resultados han arrojado hasta el momento. Después, se investigara que variables influyen en cada proceso y determinar cuales son críticas para después finalmente, establecer el modelo de variables que puedan ser monitoreadas, para poder finalmente construir los indicadores que puedan darnos información sobre los procesos de seguridad.

Después de encontrar las variables e indicadores el objetivo será determinar si las variables tienen validez dentro alguna empresa que tenga establecidos algunos de estos procesos. Principalmente el objetivo será determinar si las variables e indicadores encontrados tienen sentido dentro de los procesos y si nos arrojan alguna información sobre su estado.

## 2.9.-Riesgos de la investigación.

Los riesgos que nuestra investigación puede presentar, es que el tiempo de estudio no pueda ser el suficiente para determinar las variables critica de todos los procesos y por tanto tampoco poder obtener las métricas suficientes para determinar el; estado de los procesos.

## 2.10.-Recursos requeridos.

Para el desarrollo de esta investigación, nos apoyaremos en diferentes recursos, los cuales se describen a continuación.

**Recursos académicos.**

Necesitaremos material bibliográfico de apoyo escrito y en Internet como son: biblioteca digital, libros, revistas, posiblemente asistir a congresos, conferencias y eventos relacionados con el tema de la seguridad de la información.

**Recursos humanos.**

También necesitaremos el apoyo de todas las personas independientes y que laboren en corporaciones que estén trabajando en seguridad de información y que puedan aportar información importante en nuestra investigación. En especial el apoyo de los departamentos de sistemas de dichas corporaciones.

**Recursos materiales.**

Para validar las variables e indicadores nos apoyaremos en una corporación donde se pueda implementar el monitoreo de estas variables y poder determinar si nos arrojan los resultados deseados.

# Capitulo 3.- Mapa conceptual de procesos

***Proceso de concientización.***

## 3.1.-Introducción

La seguridad de la información es una de las mayores preocupaciones de las empresas de hoy. Conseguir que los empleados tomen conciencia del tema constituye el objetivo fundamental de un programa de sensibilización. Naturalmente, este debe formar parte de una estrategia integral que involucra: concientización propiamente dicha, entrenamiento, educación y desarrollo, todo esto orientado al logro de una ***"cultura organizacional"*** en torno al tema.

Una vez alcanzados los objetivos, el programa deberá proseguir, en forma continua, dado que este es un tema dinámico que no puede ser archivado. De igual manera, es necesario reforzar los conceptos y conductas, para que el programa sea efectivo a corto, mediano y largo plazo.

En esta sección se pretende definir indicadores que permitan establecer la eficiencia del programa y aplicar los correctivos necesarios para su adecuado funcionamiento.

Un factor importante para lograr el éxito de un programa de estas características consiste en la adecuada definición de las audiencias, donde la selección de grupos con niveles de conocimiento e intereses similares es fundamental.

## 3.2.-Barreras que enfrenta un programa de concientización.

Uno de los objetivos fundamentales que se persiguen con la implementación de un programa de concientización en seguridad es que los diferentes usuarios de los sistemas en la empresa se den cuenta de su responsabilidad en la protección de la confidencialidad, integridad y disponibilidad de los activos de información de la compañía, y que comprendan que esto no es solo competencia de los especialistas en seguridad. El programa debe perseguir dejar en claro no solo cómo proteger los sistemas sino también porqué es importante su protección y cómo los usuarios se convierten en la primera barrera de seguridad para ellos. La implementación del programa de sensibilización ayuda a minimizar los costos ocasionados por los incidentes de seguridad de

# Capitulo 3.- Mapa conceptual de procesos

***Proceso de concientización.***

## 3.1.-Introducción

La seguridad de la información es una de las mayores preocupaciones de las empresas de hoy. Conseguir que los empleados tomen conciencia del tema constituye el objetivo fundamental de un programa de sensibilización. Naturalmente, este debe formar parte de una estrategia integral que involucra: concientización propiamente dicha, entrenamiento, educación y desarrollo, todo esto orientado al logro de una ***"cultura organizacional"*** en torno al tema.

Una vez alcanzados los objetivos, el programa deberá proseguir, en forma continua, dado que este es un tema dinámico que no puede ser archivado. De igual manera, es necesario reforzar los conceptos y conductas, para que el programa sea efectivo a corto, mediano y largo plazo.

En esta sección se pretende definir indicadores que permitan establecer la eficiencia del programa y aplicar los correctivos necesarios para su adecuado funcionamiento.

Un factor importante para lograr el éxito de un programa de estas características consiste en la adecuada definición de las audiencias, donde la selección de grupos con niveles de conocimiento e intereses similares es fundamental.

## 3.2.-Barreras que enfrenta un programa de concientización.

Uno de los objetivos fundamentales que se persiguen con la implementación de un programa de concientización en seguridad es que los diferentes usuarios de los sistemas en la empresa se den cuenta de su responsabilidad en la protección de la confidencialidad, integridad y disponibilidad de los activos de información de la compañía, y que comprendan que esto no es solo competencia de los especialistas en seguridad. El programa debe perseguir dejar en claro no solo cómo proteger los sistemas sino también porqué es importante su protección y cómo los usuarios se convierten en la primera barrera de seguridad para ellos. La implementación del programa de sensibilización ayuda a minimizar los costos ocasionados por los incidentes de seguridad de

información dado que actúa directamente sobre uno de los eslabones más débiles en la cadena de seguridad, los usuarios.

La implementación de un programa exitoso de concientización en el tema de seguridad de información resulta ser una tarea bastante complicada, dado que en su camino se encuentra con una gran cantidad de obstáculos, los cuales se convierten en retos que se deben enfrentar para lograr los objetivos planteados. Dentro de estos retos se destacan los siguientes:

**Usuarios reacios al cambio.**

Dado que la tecnología ha venido evolucionando con un ritmo bastante intensivo, las empresas no siempre han podido involucrar a tiempo dentro de sus programas de capacitación los diferentes cambios que las nuevas tendencias imponen. Lo anterior ha favorecido que los usuarios hayan ido formando y fortaleciendo malos hábitos en el tema de seguridad de la información y que se muestren reacios a incorporar y adoptar nuevos comportamientos que son exigidos por los avances en tecnología y por el surgimiento de nuevas formas de ataques a los sistemas. Así, la tarea de concientización no solo deberá enfrentar el trabajo de capacitar a los usuarios en los nuevos temas sino que deberá también ayudar a erradicar las malas costumbres adquiridas por estos con respecto a la seguridad, lo cual se traduce en una doble carga de trabajo.

**No reconocer que la seguridad es un problema de todos.**

Es fácil encontrar que los trabajadores de las diferentes áreas de la empresa, y en especial de aquellas no tecnológicas, sientan que su responsabilidad se limita a las funciones asignadas a sus respectivos cargos y vean los temas de seguridad como responsabilidad exclusiva de las áreas de Tecnología de Información. El programa de concientización debe enfrentar la tarea de hacer ver a estos usuarios que el área de seguridad en la compañía no puede enfrentar sola el tema de seguridad y que requiere de la colaboración de todos los empleados. Un primer paso para esto es la definición clara, y posterior divulgación, de las políticas corporativas en torno al tema de seguridad, pero el trabajo no puede terminar allí, pues debe haber un seguimiento permanente y acciones continuadas.

**Introducción de nueva tecnología.**

Cada vez que en las empresas se adelanta un plan de renovación o actualización tecnológica generalmente se introducen cambios en el comportamiento necesario o esperado por parte de los usuarios para adaptarse a las nuevas condiciones. Con frecuencia se observa como la tecnología avanza más rápido que el ritmo de evolución de los programas de entrenamiento ocasionando que las empresas queden rezagadas o que pierdan oportunidades de capacitación interesantes brindadas por los proveedores.

**Elaboración de programas únicos.**

No todas las personas en una organización asimilan los mensajes de la misma manera. De igual forma, no todos requieren por igual conocer con la misma profundidad del tema, dado que las diferentes y variadas funciones de cada uno hacen que sus necesidades no sean idénticas. Por lo tanto, se hace necesaria una segmentación o diferenciación de audiencias, de tal forma que se envíen los mensajes de seguridad claves o necesarios para cada uno de los grupos en el lenguaje apropiado para cada uno. La elaboración y aplicación de un programa único de concientización que se aplique a todos los empleados de la empresa puede ser una estrategia fácil y rápida de implementar pero no adecuada para el logro de los objetivos de este tipo de programas.

**Bombardeo de información a los usuarios.**

Es común que la gente tienda a saturarse fácilmente cuando se presenta un bombardeo de información en torno a un tema específico, a pesar de que se haya hecho previamente una segmentación de audiencias y se estén manejando los mensajes que deben ir específicamente a cada una de ellas. Cuando lo anterior ocurre, no se logra que el mensaje llegue con la precisión necesaria y en muchas ocasiones lo que se logra es desviar la atención de la audiencia hacia temas menos sofocantes. Una práctica que puede resultar útil para no caer en el problema descrito es escuchar detenidamente a las diferentes audiencias para identificar sus necesidades específicas de entrenamiento en seguridad y poder enfocar los esfuerzos del programa de sensibilización en dichos elementos.

**No aplicar la metodología adecuada.**

Muchos de los programas de concientización en seguridad pueden fallar por la falta de consistencia en la metodología de entrenamiento implementada o porque esta no ha incluido todos los elementos o pasos necesarios para su correcta aplicación o porque estos se han desarrollado en un orden incorrecto. Estos factores pueden ser afectados igualmente por el hecho de usar canales de comunicación no adecuados para que los mensajes lleguen efectiva y oportunamente a los usuarios.

**Falla en el seguimiento del programa.**

Para que el programa de entrenamiento sea perdurable en el tiempo y se logren los resultados esperados, se requiere una permanente comunicación entre el personal especializado de seguridad y el resto de los empleados de la organización. De igual manera es necesario escuchar y recibir las sugerencias y necesidades de entrenamiento por parte de los usuarios de modo que se logren

adaptar y reforzar los programas ya existentes para que incluyan los nuevos requerimientos. El seguimiento de los programas debe prestar especial atención a la correcta aplicación de los conocimientos divulgados por parte de los usuarios y demás personal entrenado.

**Falta de apoyo por parte de la gerencia.**

Uno de los factores esenciales para el éxito de un programa de concientización es la participación activa y permanente de la alta gerencia mediante la aplicación de todas las normas establecidas y el apoyo económico necesario para la implementación de todos los planes. Cuando los niveles subordinados en la organización ven que los altos directivos efectivamente aplican y siguen todas las normas de seguridad establecidas, tal comportamiento puede ser tomado como ejemplo por parte de los demás empleados de la compañía. Por otra parte, la alta gerencia debe ser conciente de que si bien, un adecuado programa de seguridad en capacitación y en materia de tecnología implica asumir elevados costos, no lo es menos que serían mayores aquellos que tendría que asumir por la recuperación de sistemas afectados por ataques a las vulnerabilidades existentes.

**Ingeniería social.**

Esta práctica, más que afectar la implementación de un programa de concientización en seguridad, puede comprometer el éxito del mismo dado que implica directamente el enlace más débil que se trata de fortalecer que es la gente. Las personas objetivo de esta práctica suelen ser gente de confianza y muy colaboradoras en la organización (recepcionistas, asistentes administrativos, personal de mesas de ayuda, de soporte técnico, operadores de computadores, etc.) que tienen acceso a información o a procedimientos internos, en muchas ocasiones confidenciales.

Dado que esta técnica se vale de la manipulación o intimidación a las personas, resulta ser una práctica muy fácil de utilizar, de bajo costo y bastante efectiva por lo cual es de amplio uso por parte de los atacantes a los sistemas de información de las empresas. Por lo anterior es necesario incluir toda la información relacionada con este tipo de prácticas dentro de los programas de entrenamiento de tal forma que sea adecuadamente divulgada a todo el personal de la organización.

## 3.3.-Nuevas formas de inseguridad.

Dado que día a día nos encontramos con nuevos avances en materia de tecnología, tales como PDAs, Wireless, dispositivos USB, nuevos protocolos, etc., para cada uno de ellos se van presentando diversas formas de inseguridad

adaptar y reforzar los programas ya existentes para que incluyan los nuevos requerimientos. El seguimiento de los programas debe prestar especial atención a la correcta aplicación de los conocimientos divulgados por parte de los usuarios y demás personal entrenado.

**Falta de apoyo por parte de la gerencia.**

Uno de los factores esenciales para el éxito de un programa de concientización es la participación activa y permanente de la alta gerencia mediante la aplicación de todas las normas establecidas y el apoyo económico necesario para la implementación de todos los planes. Cuando los niveles subordinados en la organización ven que los altos directivos efectivamente aplican y siguen todas las normas de seguridad establecidas, tal comportamiento puede ser tomado como ejemplo por parte de los demás empleados de la compañía. Por otra parte, la alta gerencia debe ser conciente de que si bien, un adecuado programa de seguridad en capacitación y en materia de tecnología implica asumir elevados costos, no lo es menos que serían mayores aquellos que tendría que asumir por la recuperación de sistemas afectados por ataques a las vulnerabilidades existentes.

**Ingeniería social.**

Esta práctica, más que afectar la implementación de un programa de concientización en seguridad, puede comprometer el éxito del mismo dado que implica directamente el enlace más débil que se trata de fortalecer que es la gente. Las personas objetivo de esta práctica suelen ser gente de confianza y muy colaboradoras en la organización (recepcionistas, asistentes administrativos, personal de mesas de ayuda, de soporte técnico, operadores de computadores, etc.) que tienen acceso a información o a procedimientos internos, en muchas ocasiones confidenciales.

Dado que esta técnica se vale de la manipulación o intimidación a las personas, resulta ser una práctica muy fácil de utilizar, de bajo costo y bastante efectiva por lo cual es de amplio uso por parte de los atacantes a los sistemas de información de las empresas. Por lo anterior es necesario incluir toda la información relacionada con este tipo de prácticas dentro de los programas de entrenamiento de tal forma que sea adecuadamente divulgada a todo el personal de la organización.

## 3.3.-Nuevas formas de inseguridad.

Dado que día a día nos encontramos con nuevos avances en materia de tecnología, tales como PDAs, Wireless, dispositivos USB, nuevos protocolos, etc., para cada uno de ellos se van presentando diversas formas de inseguridad

como: gusanos multiplataforma, código malicioso en general, nuevas vulnerabilidades asociadas a protocolos y sistemas operativos, etc.

Estos problemas no deberían considerarse, como ocurre en muchas organizaciones, asunto exclusivo del área de tecnología, sino de toda la organización. Esto solo se logra mediante un programa de concientización que refuerce los conocimientos adquiridos en materia de seguridad y resalte las nuevas amenazas a todos los que están expuestos a ellas.

## 3.4.-Elementos claves de un programa de concientización

Inicialmente se hace claridad en tres términos que aunque responden a conceptos totalmente distintos, suelen presentar confusiones. El primero es la concientización, dentro del contexto de este documento, nos referimos a ella como a un proceso de aprendizaje que busca modificar actitudes y percepciones tanto organizacionales como individuales, con el fin de desarrollar en los usuarios una idea de la importancia de la seguridad, así como demostrar los grandes problemas que acarrea el desconocimiento o la desobediencia de las normas de seguridad. El segundo término, el entrenamiento, se considera como una etapa posterior a la concientización; este, de una manera formal construye conocimiento con el propósito de aumentar las capacidades de una persona para desarrollar sus funciones de una manera más eficiente. Por último, aparece la educación, también considerada una forma avanzada de entrenamiento, cuyo objetivo es mejorar y desarrollar conocimiento, destrezas y habilidades; el propósito de esta última es darle al empleado las habilidades necesarias para desempeñar un trabajo distinto en la organización. Algunos autores integran una cuarta categoría, el desarrollo, este tiene que ver con la transferencia de conocimientos y experiencias con el fin de abrir nuevos horizontes a los empleados.

| **Elementos de comparación** | **Concientización** | **Entrenamiento** | **Educación** |
|---|---|---|---|
| **Atributo** | ¿qué? | ¿cómo? | ¿por qué? |
| **Nivel** | Información | Conocimiento | Visión interna detallada |
| **Objetivo de aprendizaje** | Reconocimiento y retención | Destrezas | Entendimiento |
| **Ejemplos de metodología de enseñanza** | Medios (videos, cartas, afiches) | Instrucción práctica (lecturas, casos de estudio, pruebas prácticas) | Instrucción práctica (seminarios, grupos de discusión, investigación) |
| **Exámenes o pruebas de medición** | Falso/Verdadero, escogencia múltiple | Resolución de problemas | Ensayos |
| **Marco de tiempo para resultados** | Corto plazo | Mediano plazo | Largo plazo |

Tabla 2.- Comparación de actividades en concientización

como: gusanos multiplataforma, código malicioso en general, nuevas vulnerabilidades asociadas a protocolos y sistemas operativos, etc.

Estos problemas no deberían considerarse, como ocurre en muchas organizaciones, asunto exclusivo del área de tecnología, sino de toda la organización. Esto solo se logra mediante un programa de concientización que refuerce los conocimientos adquiridos en materia de seguridad y resalte las nuevas amenazas a todos los que están expuestos a ellas.

## 3.4.-Elementos claves de un programa de concientización

Inicialmente se hace claridad en tres términos que aunque responden a conceptos totalmente distintos, suelen presentar confusiones. El primero es la concientización, dentro del contexto de este documento, nos referimos a ella como a un proceso de aprendizaje que busca modificar actitudes y percepciones tanto organizacionales como individuales, con el fin de desarrollar en los usuarios una idea de la importancia de la seguridad, así como demostrar los grandes problemas que acarrea el desconocimiento o la desobediencia de las normas de seguridad. El segundo término, el entrenamiento, se considera como una etapa posterior a la concientización; este, de una manera formal construye conocimiento con el propósito de aumentar las capacidades de una persona para desarrollar sus funciones de una manera más eficiente. Por último, aparece la educación, también considerada una forma avanzada de entrenamiento, cuyo objetivo es mejorar y desarrollar conocimiento, destrezas y habilidades; el propósito de esta última es darle al empleado las habilidades necesarias para desempeñar un trabajo distinto en la organización. Algunos autores integran una cuarta categoría, el desarrollo, este tiene que ver con la transferencia de conocimientos y experiencias con el fin de abrir nuevos horizontes a los empleados.

| **Elementos de comparación** | **Concientización** | **Entrenamiento** | **Educación** |
|---|---|---|---|
| **Atributo** | ¿qué? | ¿cómo? | ¿por qué? |
| **Nivel** | Información | Conocimiento | Visión interna detallada |
| **Objetivo de aprendizaje** | Reconocimiento y retención | Destrezas | Entendimiento |
| **Ejemplos de metodología de enseñanza** | Medios (videos, cartas, afiches) | Instrucción práctica (lecturas, casos de estudio, pruebas prácticas) | Instrucción práctica (seminarios, grupos de discusión, investigación) |
| **Exámenes o pruebas de medición** | Falso/Verdadero, escogencia múltiple | Resolución de problemas | Ensayos |
| **Marco de tiempo para resultados** | Corto plazo | Mediano plazo | Largo plazo |

Tabla 2.- Comparación de actividades en concientización

La razón de la aclaración anterior dentro de este documento radica en que por sus características cada una de estas herramientas requiere de una aproximación totalmente distinta, las etapas de análisis, diseño, desarrollo, implementación y evaluación para cada una de ellas es radicalmente diferente. Por ejemplo, mientras que la medición de la efectividad de un programa de entrenamiento es evaluable inmediatamente acabado el programa, un plan de desarrollo sólo puede evaluarse mucho después, cuando las actitudes del empleado en nuevas funciones demuestren que los conocimientos adquiridos surtieron algún efecto.

Un plan completo de generación de una nueva cultura organizacional dirigida al tema de la seguridad de la información puede requerir de todas las herramientas de transmisión de conocimiento anteriores.

Es necesario revisar la existencia de programas de entrenamiento previos o en desarrollo, que pudieran servir como complemento o punto de partida, si existieran.

Algunas preguntas claves relacionadas con la seguridad informática, y que de cierta manera deben ser abordadas dentro de un plan de concientización tienen que ver con la definición de las posibles amenazas, los activos que se deben proteger y los responsables de la protección de aquellos.

- ¿Cuáles son las amenazas?
- ¿Qué se debe proteger?
- ¿Quiénes son los responsables?
- ¿Cuáles son los mecanismos de protección?

A continuación se describen algunos elementos que deben ser considerados en cualquier programa de concientización.

**Las políticas**

Las políticas de Seguridad identifican responsabilidades y establecen los objetivos para una protección apropiada y consistente de los activos de información de la organización. La implementación de las políticas busca reducir el riesgo de que en forma accidental o intencional se divulgue, modifique, destruya o haga mal uso de los activos de información y operaciones críticas. Al mismo tiempo, las políticas permiten a las áreas responsables de la administración de seguridad orientar y mejorar la administración de seguridad de los activos de información y proveer las bases para el monitoreo a través de toda la organización.

Antes de afrontar cualquier plan de concientización se deben definir primero los objetivos de la misma, y en el área de seguridad de la información estos objetivos deben responder a las políticas de seguridad de la compañía.

**Audiencias**

Aunque este podría considerarse un aspecto trivial, en muchas ocasiones marca la diferencia entre el éxito y el fracaso del programa.

En el ámbito de las audiencias, es importante la conformación de grupos objetivo. La definición de dichos grupos no obedece a una regla estricta. Más bien, cada caso debe ser considerado de manera particular. Esta decisión puede estar determinada por razones tan diversas como: las propias políticas de la organización, el tipo de organización, el ambiente laboral, el tipo de negocio, etc.

Estos grupos deberán estar integrados de manera homogénea para facilitar la participación activa de todos los individuos. En las sesiones se debe buscar la comodidad y receptividad de todos los participantes.

Estos son algunos criterios que pueden servir cono referencia para la conformación de los grupos:

**Nivel de conocimiento tecnológico**

Esta clasificación permitirá definir temas de acuerdo con las destrezas de los participantes. Hacerlo de este modo garantiza que los usuarios con menores conocimientos no se van a sentir perdidos frente al grupo. De modo recíproco, los usuarios técnicos no estarán fuera de lugar, en charlas con un contenido superficial, que no cubre sus expectativas.

En esta categoría, los grupos pueden ser:

Administradores: pueden incluir administradores de aplicaciones, bases de datos, sistemas operativos y dispositivos.

Usuarios avanzados: esta categoría permite agrupar a usuarios con diferentes niveles de destreza en tecnologías de la información, que no realizan labores de administración, pero con algunas características particulares en función del rol que desempeñan, por ejemplo el empleado del área de Recursos Humamos que no posee un conocimiento técnico avanzado, pero es el propietario de los datos y tiene acceso a estos de manera amplia.

Usuarios con muy pocas destrezas técnicas: todos aquellos no contemplados en las otras categorías.

**Nivel jerárquico**

En ocasiones puede ser necesario agrupar las audiencias según la jerarquía. Esto permite orientar los temas de acuerdo con los intereses de cada grupo, concentrándose en objetivos específicos para cada nivel dentro de la compañía.

Ejecutivos: son los encargados de planificar, dirigir, ejecutar y controlar las políticas, estrategias y directrices corporativas, así como presentar al nivel directivo los proyectos. Aprueban los planes de desarrollo a largo plazo

Directivos: son los encargados de fijar las políticas, estrategias y directrices corporativas y velar por su cumplimiento. Aprueban y administran el presupuesto.

Administrativos: constituido por las áreas o individuos que brindan asistencia administrativa para la ejecución de los programas, planes y proyectos, de acuerdo con sus funciones.

Operativos: son las áreas o individuos encargados de realizar las labores relacionadas con el funcionamiento diario del negocio y toda la logística asociada.

**Nivel de sensibilidad en temas de seguridad de la información y a la tecnología**

Muy sensibles y dispuestos al cambio: son individuos que por la naturaleza de su trabajo, o su propia naturaleza, tienen inclinación a apoyar el programa. Se debe aprovechar su actitud para convertirlos en aliados y motor del cambio.

Nivel medio de sensibilidad: su participación es decisiva. Habitualmente, constituyen el grupo más numeroso. Si se logra convertirlos en aliados, seguramente contribuirá al éxito del programa, en caso contrario, dificultarán el desarrollo del proyecto, llegando incluso a impedirlo.

Apatía, desinterés o rechazo: este grupo debe ser abordado con mucho tacto, pues de no hacerlo así y lograr convertirlos en aliados, podrían arrastrar a los del nivel medio y convertirse en una fuerza incontenible que acabaría con el proyecto.

## 3.5.-Nivel de acceso a la información y a los recursos de tecnológicos

Administradores: usuarios que tienen prácticamente el control total de la información, con gran destreza técnica.

Usuarios con privilegios especiales: usuarios que a pesar de no tener amplios conocimientos técnicos, en virtud de su posición dentro de la organización,

**Nivel jerárquico**

En ocasiones puede ser necesario agrupar las audiencias según la jerarquía. Esto permite orientar los temas de acuerdo con los intereses de cada grupo, concentrándose en objetivos específicos para cada nivel dentro de la compañía.

Ejecutivos: son los encargados de planificar, dirigir, ejecutar y controlar las políticas, estrategias y directrices corporativas, así como presentar al nivel directivo los proyectos. Aprueban los planes de desarrollo a largo plazo

Directivos: son los encargados de fijar las políticas, estrategias y directrices corporativas y velar por su cumplimiento. Aprueban y administran el presupuesto.

Administrativos: constituido por las áreas o individuos que brindan asistencia administrativa para la ejecución de los programas, planes y proyectos, de acuerdo con sus funciones.

Operativos: son las áreas o individuos encargados de realizar las labores relacionadas con el funcionamiento diario del negocio y toda la logística asociada.

**Nivel de sensibilidad en temas de seguridad de la información y a la tecnología**

Muy sensibles y dispuestos al cambio: son individuos que por la naturaleza de su trabajo, o su propia naturaleza, tienen inclinación a apoyar el programa. Se debe aprovechar su actitud para convertirlos en aliados y motor del cambio.

Nivel medio de sensibilidad: su participación es decisiva. Habitualmente, constituyen el grupo más numeroso. Si se logra convertirlos en aliados, seguramente contribuirá al éxito del programa, en caso contrario, dificultarán el desarrollo del proyecto, llegando incluso a impedirlo.

Apatía, desinterés o rechazo: este grupo debe ser abordado con mucho tacto, pues de no hacerlo así y lograr convertirlos en aliados, podrían arrastrar a los del nivel medio y convertirse en una fuerza incontenible que acabaría con el proyecto.

## 3.5.-Nivel de acceso a la información y a los recursos de tecnológicos

Administradores: usuarios que tienen prácticamente el control total de la información, con gran destreza técnica.

Usuarios con privilegios especiales: usuarios que a pesar de no tener amplios conocimientos técnicos, en virtud de su posición dentro de la organización,

tienen acceso privilegiado a información sensible.

Usuarios finales: todos los demás usuarios no clasificados en ninguno de los grupos anteriores.

**Sistema operativo, aplicación o plataforma utilizada**

Aplicaciones de misión crítica: son los diferentes usuarios que tienen acceso a aplicaciones que forman parte del núcleo de negocio de la compañía.

Aplicaciones ofimáticas: usuarios de aplicaciones comunes de apoyo tales como procesadores de palabra, hojas de cálculo, etc.

Sistemas operativos de servidor o estaciones cliente: en ambientes heterogéneos en los cuales se utilizan diversas plataformas computacionales, puede ser importante dividir a los usuarios según este criterio, debido a que algunos conceptos pueden no aplicar en uno u otro caso.

Bases de datos misionales: el acceso a la información almacenada en las bases de datos asociadas a las aplicaciones que reúnen el núcleo del negocio, puede definir otro criterio de clasificación.

Consideraciones tecnológicas relacionadas con el tipo de red a la cual se tiene acceso.

LAN: los usuarios que se encuentran dentro de los confines de la red corporativa pueden tener características o necesidades comunes.

WAN: estos usuarios presentan características especiales que deben ser tenidas en cuenta tales como acceso a Internet y Extranets, lo cual los hace más vulnerables.

Wireless: una de las tecnologías con mayores índices de crecimiento en la actualidad y de mayor proyección. Representa un gran reto en materia de seguridad.

**Apoyo por parte de la alta gerencia**

Naturalmente, todos los elementos mencionados en este trabajo son importantes para el éxito del programa. Sin embargo, el apoyo por parte de la alta gerencia es crucial, sin el, las probabilidades de lograr la meta propuesta serán prácticamente nulas.

Todos los empleados de la organización podrán responder de una manera más efectiva y con mayor grado de compromiso, si sienten que el programa es importante para lograr los objetivos de negocio, y hace parte de la misión. Será más probable lograr el éxito del programa con la participación de la alta y media gerencia.

Con el fin de lograr la participación de la gerencia se debe entregar: un análisis costo/beneficio del proyecto; necesidades, por parte de la empresa, de soporte a

estándares internacionales y mejores prácticas de la industria; cumplimiento de requerimientos legales y de auditoria y análisis de riesgos, entre otros.

Es conveniente entregar un informe ejecutivo que contenga los principales retos que debe enfrentar el programa, la forma de afrontarlos y las metas propuestas. Este resumen también debe contener una descripción del plan de implementación, presentado como una actividad permanente y dinámica en el tiempo, que pueda ser actualizada con la periodicidad requerida, y no como algo puntual y estático. El tema se debe cerrar mencionando las necesidades logísticas y presupuestales del proyecto.

Aunque es posible llevar a cabo un programa de esta naturaleza sin los elementos mencionados, no se puede ser muy optimista respecto al logro de los objetivos propuestos, en estas condiciones.

El apoyo de la gerencia contribuye, de manera decisiva, en los siguientes aspectos:

Consecución de recursos necesarios: aquí se consideran recursos financieros, de personal, y en general, aspectos de logística.

Compromiso de los empleados: si no se cuenta con este apoyo, es probable que individuos o áreas de un alto nivel jerárquico no se sientan comprometidas y no participen de manera activa, llegando incluso a entorpecer el desarrollo del programa.

Agilizar los procesos: tanto internos (de la propia organización) como con terceros, para reducir los tiempos de inactividad que pueden poner en riesgo el éxito del programa. Estos eventos deben ser incluidos en la matriz de riesgos del proyecto para buscar una estrategia de mitigación.

Facilitar el seguimiento: asistiendo y promoviendo la asistencia de todos los involucrados a las reuniones programadas y la revisión del cronograma para determinar el cumplimiento de objetivos, dentro de lo presupuestado.

### 3.6.-Mecanismos de comunicación

Los entornos empresariales de hoy cuentan con gran cantidad de medios de comunicación y difusión, los cuales pueden ser aprovechados para lograr un mayor impacto. No obstante, no se debe abusar pues esto puede conducir a saturación de la audiencia, produciendo resultados adversos.

estándares internacionales y mejores prácticas de la industria; cumplimiento de requerimientos legales y de auditoria y análisis de riesgos, entre otros.

Es conveniente entregar un informe ejecutivo que contenga los principales retos que debe enfrentar el programa, la forma de afrontarlos y las metas propuestas. Este resumen también debe contener una descripción del plan de implementación, presentado como una actividad permanente y dinámica en el tiempo, que pueda ser actualizada con la periodicidad requerida, y no como algo puntual y estático. El tema se debe cerrar mencionando las necesidades logísticas y presupuestales del proyecto.

Aunque es posible llevar a cabo un programa de esta naturaleza sin los elementos mencionados, no se puede ser muy optimista respecto al logro de los objetivos propuestos, en estas condiciones.

El apoyo de la gerencia contribuye, de manera decisiva, en los siguientes aspectos:

Consecución de recursos necesarios: aquí se consideran recursos financieros, de personal, y en general, aspectos de logística.

Compromiso de los empleados: si no se cuenta con este apoyo, es probable que individuos o áreas de un alto nivel jerárquico no se sientan comprometidas y no participen de manera activa, llegando incluso a entorpecer el desarrollo del programa.

Agilizar los procesos: tanto internos (de la propia organización) como con terceros, para reducir los tiempos de inactividad que pueden poner en riesgo el éxito del programa. Estos eventos deben ser incluidos en la matriz de riesgos del proyecto para buscar una estrategia de mitigación.

Facilitar el seguimiento: asistiendo y promoviendo la asistencia de todos los involucrados a las reuniones programadas y la revisión del cronograma para determinar el cumplimiento de objetivos, dentro de lo presupuestado.

### 3.6.-Mecanismos de comunicación

Los entornos empresariales de hoy cuentan con gran cantidad de medios de comunicación y difusión, los cuales pueden ser aprovechados para lograr un mayor impacto. No obstante, no se debe abusar pues esto puede conducir a saturación de la audiencia, produciendo resultados adversos.

Entre los medios y mecanismos que pueden ser utilizados se encuentran:

Correo electrónico: es, hoy por hoy, el medio de mayor cobertura en la mayoría de las organizaciones que cuentan con tecnología. Es eficaz, económico, ágil y permite alcanzar a las áreas o empleados que se hayan geográficamente dispersos y que serían virtualmente inalcanzables por otros medios.

Intranet: otro recurso tecnológico importante. Tiene la ventaja, sobre el correo, de favorecer la posibilidad de utilizar documentos más ricos en contenido, incluyendo multimedia, sin afectar de manera importante los recursos y el funcionamiento de la red.

Carteleras y volantes: si bien cada día las compañías soportan más y más procesos en tecnología, no todos los empleados son usuarios de la misma. Pese a esto, la información concierne a todos. Estos medios llegarán a usuarios que no tienen acceso a la tecnología, con quienes no se podría utilizar otro tipo de medios o mecanismos. Para aquellos que tienen acceso a la tecnología, deben considerarse como un complemento.

Login de acceso a la red: dado que este es el punto central de acceso a los recursos tecnológicos, constituye un recurso que puede ser explotado exitosamente. La restricción que impone es el tamaño de los mensajes que se pueden difundir a través de este medio. Su importancia radica en el hecho de que se puede forzar a todos los empleados a recibirlo y a la frecuencia con la cual se entregan los mensajes.

Concursos: constituyen una forma de despertar el interés y la sana competencia. Si se pueden explotar, generalmente permiten alcanzar niveles muy altos de éxito y pueden contribuir a lograr un clima organizacional de cooperación y trabajo en equipo.

Reuniones y conferencias: con la participación de expertos se puede consolidar el trabajo realizado por los empleados de la organización y llamar la atención de los más reacios, para vincularlos al proceso.

Memorandos y documentos de comunicación interna: si bien no constituyen el medio por excelencia para esta clase de objetivos, no deben ser desestimados. Su importancia radica en el carácter formal, el cual genera un mayor nivel de compromiso por parte de todos los involucrados. Si se utilizan, debe tenerse especial cuidado de no abusar de ellos.

Artículos y publicaciones especializadas: pueden ser útiles particularmente para los usuarios de tecnología con conocimientos más profundos en el tema.

Su propósito debe ser reforzar el trabajo hecho utilizando otros medios y mecanismos.

### 3.7.-Metodología adecuada

En esta parte se describirán planes dirigidos a la definición de las iniciativas anteriores. Se revisará principalmente una metodología establecida con este fin, y la posibilidad de complementar algunos de sus puntos con guías de organismos internacionales.

Inicialmente se comenzará por revisar algunos elementos importantes, los cuales llevan a la selección de una metodología particular.

Primero, la seguridad es un tema que involucra a toda una organización, y debe ser tratada como algo integral; cuando se habla de toda la organización, es para referirse a un sistema bastante complejo con unas entradas, unos procesos internos y finalmente unas salidas.

Segundo, y como consecuencia de lo anterior, las estrategias de concientización y entrenamiento deben ser revisadas dentro del contexto de sistemas, donde los usuarios hacen parte de un todo, y los conocimientos impartidos deben responder a una política integral o general.

Basándose en lo anterior, se decidió presentar la metodología conocida como Diseño de Sistemas de Instrucción (ISD por sus siglas en inglés). Esta metodología afronta la problemática desde un punto general, y revisa cada unos de los componentes de la transmisión del conocimiento: definición de objetivos, material, audiencia y métodos de evaluación, desde ese punto de vista. La metodología además garantiza un uso consciente de los recursos destinados para la capacitación.

El ISD plantea las siguientes etapas para la definición de este tipo de planes:

Análisis: Es el primer paso, y su resultado es una clara definición de las audiencias, los contenidos y las razones que sustentan lo anterior. Consiste en la recolección de datos, y su posterior análisis; e incluye entrevistas individuales, grupos de trabajo, observación, y el estudio de los materiales a utilizar dentro del plan de capacitación. Posteriormente se revisarán algunas guías más específicas para una definición más exacta en el tema de las audiencias. En esta etapa se comienza con la definición de los medios que se utilizarán para impartir la capacitación y se revisa cualquier inconveniente que pudiese presentarse con la puesta en marcha de los programas. De acuerdo con lo dicho anteriormente, el ISD tiene un enfoque sistémico, y es precisamente en esta

Su propósito debe ser reforzar el trabajo hecho utilizando otros medios y mecanismos.

### 3.7.-Metodología adecuada

En esta parte se describirán planes dirigidos a la definición de las iniciativas anteriores. Se revisará principalmente una metodología establecida con este fin, y la posibilidad de complementar algunos de sus puntos con guías de organismos internacionales.

Inicialmente se comenzará por revisar algunos elementos importantes, los cuales llevan a la selección de una metodología particular.

Primero, la seguridad es un tema que involucra a toda una organización, y debe ser tratada como algo integral; cuando se habla de toda la organización, es para referirse a un sistema bastante complejo con unas entradas, unos procesos internos y finalmente unas salidas.

Segundo, y como consecuencia de lo anterior, las estrategias de concientización y entrenamiento deben ser revisadas dentro del contexto de sistemas, donde los usuarios hacen parte de un todo, y los conocimientos impartidos deben responder a una política integral o general.

Basándose en lo anterior, se decidió presentar la metodología conocida como Diseño de Sistemas de Instrucción (ISD por sus siglas en inglés). Esta metodología afronta la problemática desde un punto general, y revisa cada unos de los componentes de la transmisión del conocimiento: definición de objetivos, material, audiencia y métodos de evaluación, desde ese punto de vista. La metodología además garantiza un uso consciente de los recursos destinados para la capacitación.

El ISD plantea las siguientes etapas para la definición de este tipo de planes:

Análisis: Es el primer paso, y su resultado es una clara definición de las audiencias, los contenidos y las razones que sustentan lo anterior. Consiste en la recolección de datos, y su posterior análisis; e incluye entrevistas individuales, grupos de trabajo, observación, y el estudio de los materiales a utilizar dentro del plan de capacitación. Posteriormente se revisarán algunas guías más específicas para una definición más exacta en el tema de las audiencias. En esta etapa se comienza con la definición de los medios que se utilizarán para impartir la capacitación y se revisa cualquier inconveniente que pudiese presentarse con la puesta en marcha de los programas. De acuerdo con lo dicho anteriormente, el ISD tiene un enfoque sistémico, y es precisamente en esta

fase en donde se identifican los sistemas que componen la empresa, con base en esta definición se hace la revisión de materiales, métodos de enseñanza, etc.

Diseño: Consiste en la definición de los temas a ser desarrollados en el curso. Incluye los siguientes temas:

Desarrollo y definición de objetivos de aprendizaje para cada tarea.

Identificación de métodos de evaluación.

Identificación de métodos de distribución.

Creación de guías de flujo de información y organización, además de materiales y actividades.

La primera tarea es la definición de los objetivos, en la que además se definen los criterios para medir el éxito de los participantes en la consecución de los mismos. La capacitación debe responder a tres tipos distintos de funciones o necesidades, que tienen que ver con la necesidad de consecución de conocimiento, las destrezas y las habilidades. Dependiendo de la necesidad de la audiencia, de acuerdo con la división anterior, se deben diseñar los materiales, la metodología y los métodos de evaluación.

En la segunda fase, la de la identificación de los métodos de evaluación, se desarrollan los respectivos criterios de evaluación, basándose en los objetivos de aprendizaje del programa. Durante esta etapa del proceso es importante crear el plan de evaluación, de manera que quede perfectamente integrada con el material del curso. Es importante identificar y crear métodos de evaluación que soporten la misión de la organización.

Desarrollo: Esta fase del proceso incluye la creación y afinamiento de los materiales que deben usarse durante el proceso de instrucción. Otras actividades que se incluyen en esta fase son:

- Creación de los materiales para entrenamiento de entrenadores, si aplica.
- Creación del material para los estudiantes.
- Desarrollo de laboratorios para prácticas dentro del proceso de instrucción en los casos en que aplique.

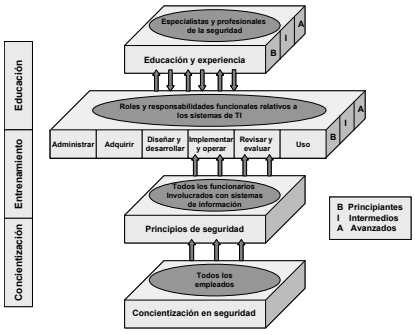



Figura 3.- Planes de instrucción en el área de seguridad

Implementación: Es la cuarta fase del proceso, e incluye las etapas necesarias para llevar a cabo el proceso de instrucción. A continuación se detallan tres actividades que hacen parte de este proceso:

- Preparación de un plan de entrenamiento maestro que se convierta en una guía para las actividades de implementación.
- Preparar los equipos, aulas y materiales.
- Desarrollar programas pilotos con la audiencia objetivo.

Evaluación y mantenimiento: Esta etapa tiene que ver con el mantenimiento y la medición de estándares de control de calidad. En ella debe asegurarse que existe una completa transferencia de conocimientos y destrezas del ambiente de capacitación al de trabajo. Los principales asuntos que deben tenerse en cuenta durante la fase de evaluación son:

- Si se logró el cambio deseado en el desempeño de los empleados.
- Si se logró con la capacitación el alcance de los objetivos por parte de los empleados.
- Alcanzó la capacitación las expectativas o necesidades de los empleados.

Aunque el modelo ISD hace especial énfasis en la correcta definición de las audiencias, deja muy abierta al usuario la conformación de las mismas. Además, otro punto importante, y que tampoco es explícito dentro del ISD es la definición de los temas para cada una de las distintas audiencias. Ambos temas se encuentran ampliamente desarrollados dentro del NIST SP 800-50 (y su predecesor, el 800-16).

El NIST SP 800-16 es otro modelo formal para el diseño de planes de instrucción en el área de seguridad. La figura que aparece a continuación muestra un diagrama del modelo.

La mayor parte de información de este proceso fue obtenida de un trabajo realizado en la universidad de los Andes Colombia y dirigido por Jeimy Cano Martínez.

### 3.8.-Métricas e Indicadores

Las variables generales encontradas en la teoría para el proceso de concientizacion se listan a continuación:

Implementación: Es la cuarta fase del proceso, e incluye las etapas necesarias para llevar a cabo el proceso de instrucción. A continuación se detallan tres actividades que hacen parte de este proceso:

- Preparación de un plan de entrenamiento maestro que se convierta en una guía para las actividades de implementación.
- Preparar los equipos, aulas y materiales.
- Desarrollar programas pilotos con la audiencia objetivo.

Evaluación y mantenimiento: Esta etapa tiene que ver con el mantenimiento y la medición de estándares de control de calidad. En ella debe asegurarse que existe una completa transferencia de conocimientos y destrezas del ambiente de capacitación al de trabajo. Los principales asuntos que deben tenerse en cuenta durante la fase de evaluación son:

- Si se logró el cambio deseado en el desempeño de los empleados.
- Si se logró con la capacitación el alcance de los objetivos por parte de los empleados.
- Alcanzó la capacitación las expectativas o necesidades de los empleados.

Aunque el modelo ISD hace especial énfasis en la correcta definición de las audiencias, deja muy abierta al usuario la conformación de las mismas. Además, otro punto importante, y que tampoco es explícito dentro del ISD es la definición de los temas para cada una de las distintas audiencias. Ambos temas se encuentran ampliamente desarrollados dentro del NIST SP 800-50 (y su predecesor, el 800-16).

El NIST SP 800-16 es otro modelo formal para el diseño de planes de instrucción en el área de seguridad. La figura que aparece a continuación muestra un diagrama del modelo.

La mayor parte de información de este proceso fue obtenida de un trabajo realizado en la universidad de los Andes Colombia y dirigido por Jeimy Cano Martínez.

### 3.8.-Métricas e Indicadores

Las variables generales encontradas en la teoría para el proceso de concientizacion se listan a continuación:

Tabla 3.- Variables e indicadores del proceso de concientización.

| Variables | Descripción. |
|---|---|
| **Xcon1**<br>Frecuencia:<br>6 Meses | Número de empleados Totales de la organización.<br>Objetivo.- Considera el número total de empleados de la organización para realizar estadísticas en base a ese número |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xcon2**<br>Frecuencia:<br>6 Meses | Período de tiempo en que se realizan las revisiones o auditorias al proceso de concientización en promedio será 6 meses<br>Objetivo.- Establece un período de tiempo específico para realizar las revisiones o auditorias del proceso de concientización en promedio será 6 meses |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xcon3**<br>Frecuencia:<br>6 Meses | Número de empleados que reciben capacitación sobre concientización en un período de 6 meses<br>Objetivo.- Determinar el porcentaje de la población total de empleados que reciben capacitación en concientización |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xcon4**<br>Frecuencia:<br>6 Meses | Número de Actividades de concientización que se realizan en un período de 6 meses<br>Objetivo.- Determina si el número de actividades que pueden ser campañas, programas, cursos, conferencias que se realizan en un período de tiempo son suficientes |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xcon5**<br>Frecuencia:<br>6 Meses | Número de audiencias creadas para las diferentes actividades de concientización en un período de 6 meses<br>Objetivo.- Determina si se han creado suficientes números de audiencias para cubrir las necesidades especificas en determinados tipos de empleados |
| Fuente: Personal | |
| **Xcon6**<br>Frecuencia:<br>6 Meses | Número de empleados que asisten por audiencia en un período de 6 meses.<br>Objetivo.- Determinar el porcentaje total de empleados de determinada área que asisten por audiencia. |
| Fuente: Personal | |
| **Xcon7**<br>Frecuencia:<br>6 Meses | Número total de tópicos que buscan revisarse en las actividades de concientización.<br>Objetivo.- Determinar el número total de tópicos que quieren revisarse en los cursos de capacitación. |
| Fuente: Personal | |

| | |
|---|---|
| **Xcon8**<br>Frecuencia:<br>6 Meses | Número de tópicos que realmente se ven en las actividades de concientización.<br>Objetivo: Determinar el número de tópicos que se ven en las actividades de concientización. |
| Fuente: Personal | |
| **Xcon9**<br>Frecuencia:<br>6 Meses | Número de actividades de concientización a las que asiste un empleado en un período de 6 meses.<br>Objetivo.- Determinar el número de actividades totales a las que asistió un empleado |
| Fuente: Personal | |
| **Xcon10**<br>Frecuencia:<br>6 Meses | Total de horas que dura un empleado en entrenamiento en un período de 6 meses<br>Objetivo: Tener el número total de horas de entrenamiento que recibe un empleado |
| Fuente: Personal | |
| **Xcon11**<br>Frecuencia:<br>6 Meses | Número total de empleados que asisten a mas horas de entrenamiento en actividades de concientización<br>Objetivo.- Determinar el número de horas promedios a las que asisten los empleados a actividades de concientización |
| Fuente: Personal | |
| **Xcon12**<br>Frecuencia:<br>6 Meses | Número de empleados que presentan las encuestas y exámenes de concientización en un período de 6 meses<br>Objetivo: Determina el número de empleados total que presentan las encuestas y exámenes |
| Fuente: Corporate information security working group | |
| **Xcon13**<br>Frecuencia:<br>6 Meses | Número de empleados que contestan correctamente las encuestas de concientización en un período de 6 meses<br>Objetivo.- Determinar que la cantidad de empleados que contestan correctamente las encuestas y exámenes |
| Fuente: Corporate information security working group | |
| **Xcon14**<br>Frecuencia:<br>6 Meses | Número de reportes de incidentes levantados en un período de 6 meses<br>Objetivo: Determina en que porcentaje hay un incremento o disminución de reportes de incidentes de seguridad debido al proceso de concientización |
| Fuente: Personal | |
| **Xcon15**<br>Frecuencia:<br>6 Meses | Número de personas que han tomado cursos de concientización y que levantaron reporte de incidentes en un período de 6 meses<br>Objetivo.- Expresa el número de personas concientizadas que levantan reportes de inseguridad |
| Fuente: Personal | |

Algunas métricas (indicadores) que podemos construir a partir de estas variables son los siguientes.

| Indicadores | Descripción. |
|---|---|
| INDCon1 | Porcentaje de personal sometido a cursos de concientización<br>Fórmula = (Xcon3*100)/Xcon1 |
| | |
| INDCon2 | Actividades de concientizacion periódicas (cada 6 meses)<br>Fórmula = Xcon4 |
| | |
| INDCon3 | Audiencias creadas por período de tiempo (5 meses)<br>Fórmula = Xcon5 |
| | |
| INDCon4 | Porcentaje de personas en determinada área que asiste por audiencia periódicamente (6 meses)<br>Fórmula = (Xcon6*100)/número total de empleados de determinada área. |
| | |
| INDCon5 | Porcentaje de cubrimiento de los tópicos en actividades de concientizacion<br>Fórmula = Con8*100/Xcon7 |
| | |
| INDCon6 | Número de horas promedio que dura un empleado en actividades de concientización<br>Fórmula = Xcon10*Xcon9 (Esta métrica es por empleado) |
| | |
| INDCon7 | Número total de empleados que asisten a mas horas de entrenamiento en actividades de concientización<br>Fórmula = Xcon11 |
| | |
| INDCon8 | Porcentaje de personas que aprueban las encuestas<br>Fórmula = (Xcon13*100)/Xcon12 |
| | |
| INDCon9 | Porcentaje de incremento o disminución de reportes de incidentes que se levantaron periódicamente (cada 6 meses)<br>Fórmula = Xcon14 – (Número del último reporte de incidentes) |
| | |
| INDCon10 | Número de personas que han tomado cursos de concientización y que levantan reportes de incidentes<br>Fórmula = Xcon15 |

## *Plan de continuidad del negocio*

### 3.9.-Introducción

Cada vez más la informatización de las empresas ayuda a progresar y mejorar su eficacia y sus objetivos como entidad y negocio. Unos servicios informáticos eficaces y efectivos son hoy en día elementos esenciales en la evolución de un negocio.

Es por ello por lo que si sucede un desastre informático esto supone como consecuencia grandes pérdidas económicas, períodos de inactividad que pueden ser largos y elevados costes. Por ello, son necesarios sistemas y servicios que ayuden a recuperar información técnica, organizativa y de funcionamiento básica para la empresa. La buena aplicación de estos servicios y soluciones de continuidad y recuperación están pensados para garantizar una total disponibilidad de los procesos esenciales del negocio.

Aunque las pérdidas por un desastre informático puedan ser muy importantes, cada vez son mayores los avances tecnológicos que permiten y hacen posible la recuperación en muy poco tiempo y a unos costes razonables, siendo sus ciclos de implantación cada vez más cortos. Sin embargo, más allá de la recuperación son necesarios servicios de continuidad del negocio que ayuden a evolucionar al sistema de un negocio.

Para dejar un poco mas claro sobre los aspectos que comprende este proceso empezaremos por definir la estructura de este proceso, así como su evolución a través del tiempo (IBM S/F).

### 3.9.1 Administración de la continuidad del negocio (BCM)

la gestión de la continuidad del negocio o Business Continuity Management (BCM), un programa que asegura la reducción prudente del riesgo y reasume las operaciones de negocio dominantes antes de que se incurra en impactos y pérdidas inaceptables(Mandujano Manuel, 2005).

El BCM deja atrás el plan de continuidad de procesos críticos (business continuity planning) de hace diez años y los planes de recuperación de desastres (disaster recovery planning) de hace 20(Mandujano Manuel, 2005).

El BCM se define como:

Un proceso administrativo holístico que identifica impactos potenciales que amenazan a una organización y proveen una estructura con la capacidad para

dar una respuesta efectiva que asegure los intereses de los stakeholders, la reputación, la marca y las actividades que crean valor.

Este debe ser un plan que se debe considerar a nivel corporativo y debe ser apoyado por todos los miembros, ya que si se carece del apoyo el proceso no tendrá éxito (Mandujano Manuel, 2005).

## 3.9.2.-Pasos del BCM

Los pasos más importantes en los que se desarrolla el BCM son los siguientes.

**Analiza tu negocio.**

En este punto es importante tomar una radiografía a la organización, así como también a la relación con los proveedores y clientes. Es importante en esta parte también determinar en que grado las personas de la empresa pueden apoyar este proceso. Otro aspecto es analizar donde la organización es vulnerable.

**Valora los riesgos**

Hay dos preguntas que se deben hacer en esta etapa.

¿Cómo seria si pasara que?
¿Qué efecto tendría en el negocio?

En este aspecto se puede definir una valoración en términos de costo: ¿cuanto podrías perder si en una emergencia tu negocio para por días, semanas o meses?, ¿Cómo reaccionarían tus clientes, proveedores e inversionistas si no estuvieras preparado para ese incidente?, ¿afectaría tu imagen?

Hay tres tipos de preguntas que se pueden manejar.

¿Que pasaría si?
¿Cuál es el peor escenario?
¿Qué funciones y personas son esenciales y cuando?

Desarrolla tu estrategia.

Independientemente del negocio que sea se debe definir una estrategia la cual puede ser alguna de las siguientes.

- aceptar el riesgo y no cambiar nada.

- aceptar el riesgo y hacer un arreglo con algún negocio o forma consultora en continuidad del negocio y obtener ayude después del incidente, el negocio puede ser además algún competidor.
- intentar reducir los riesgos.
- administrar los riesgos y hacer arreglos después del incidente.
- reducir los riesgos al punto que necesites ayuda externa.

**Desarrolla tu plan.**

Un plan debe variar dependiendo del negocio sin embargo hay algunas características en común.

Configuración.

- hacerlo claro y que lo has consultado a través de toda la empresa.
- no usar lenguajes técnicos que nadie puede entender.

Contenido

- hacerlo claro, saber quien necesita hacer que, y quien toma la responsabilidad de que, deben existir roles bien definidos.
- usar listas que los lectores puedan leer y entender rápidamente.
- incluir instrucciones claras y directas para la primera hora después del accidente.
- incluir cosas que no se pueden hacer
- el plan debe ser mantenido, actualizado y auditado.

**Ensaya tu plan**

Algunas veces tu pueden encontrar debilidades solo si puedes ensayar tu plan, el ensayar tu plan te puede ayudar a encontrar y corregir errores para lograr un plan mas flexible y robusto.

Formas posibles de ensayar tu plan.

- lee el documento al grupo y contesta a tus preguntas, escucha las sugerencias y estudia las reacciones que ellos puedan tener.
- Telefonea a los involucrados para revisar si no se pierde la comunicación o si sus datos como nombres y teléfonos están correctos.
- si existe la posibilidad realicen ensayos generales.

## 3.10.-Desarrollando un plan de continuidad del negocio

El corazón del proceso del BCM es el BCP (Plan de continuidad del negocio) este documento contiene las acciones que se pueden realizar después de un

- aceptar el riesgo y hacer un arreglo con algún negocio o forma consultora en continuidad del negocio y obtener ayude después del incidente, el negocio puede ser además algún competidor.
- intentar reducir los riesgos.
- administrar los riesgos y hacer arreglos después del incidente.
- reducir los riesgos al punto que necesites ayuda externa.

**Desarrolla tu plan.**

Un plan debe variar dependiendo del negocio sin embargo hay algunas características en común.

Configuración.

- hacerlo claro y que lo has consultado a través de toda la empresa.
- no usar lenguajes técnicos que nadie puede entender.

Contenido

- hacerlo claro, saber quien necesita hacer que, y quien toma la responsabilidad de que, deben existir roles bien definidos.
- usar listas que los lectores puedan leer y entender rápidamente.
- incluir instrucciones claras y directas para la primera hora después del accidente.
- incluir cosas que no se pueden hacer
- el plan debe ser mantenido, actualizado y auditado.

**Ensaya tu plan**

Algunas veces tu pueden encontrar debilidades solo si puedes ensayar tu plan, el ensayar tu plan te puede ayudar a encontrar y corregir errores para lograr un plan mas flexible y robusto.

Formas posibles de ensayar tu plan.

- lee el documento al grupo y contesta a tus preguntas, escucha las sugerencias y estudia las reacciones que ellos puedan tener.
- Telefonea a los involucrados para revisar si no se pierde la comunicación o si sus datos como nombres y teléfonos están correctos.
- si existe la posibilidad realicen ensayos generales.

## 3.10.-Desarrollando un plan de continuidad del negocio

El corazón del proceso del BCM es el BCP (Plan de continuidad del negocio) este documento contiene las acciones que se pueden realizar después de un

accidente, quienes son los involucrados en esas acciones y donde pueden ser contactados. el plan debe reflejar la posición de la organización y de sus stakeholders (BCI, S/F).

**Definición**

*Plan de Continuidad de Negocio* (BCP, Business Continuity Plan): Conjunto de tareas que permite a las organizaciones continuar su actividad en la situación de que un evento afecte sus operaciones. Un plan de continuidad afecta tanto a los sistemas informáticos como al resto de procesos de una organización y tiene en cuenta la situación antes, durante y después de un incidente.

**Dificultades para implantar un Plan de Continuidad de Negocio**

-Falta de Compromiso de la Dirección
-Los programas particulares no se integran entre sí
-En el diseño del plan no se realiza una gestión correcta del riesgo
-No se realizan simulacros o planes de prueba completos

**Relación entre los planes de continuidad de negocio y los sistemas de gestión de la seguridad de la información**

Tanto las normas de IT Governance como los estándares de gestión de seguridad de la información hacen referencia a la continuidad de negocio, sin embargo los BCP tienen elementos diferenciales.

En primer lugar los SGSI (Sistemas de Gestión de la Seguridad de la Información) hacen fundamentalmente referencia a la información y a los activos que la gestionan, mientras que los BCP incluyen todos los procesos esenciales de la entidad.

En segundo lugar, los SGSI trabajan fundamentalmente mediante un análisis coste/riesgo mientras que los BCP tienen como referencia fundamental el tiempo máximo que un proceso puede estar detenido sin afectar a la organización.

## 3.10.1.-Elementos de un Plan de Continuidad de Negocio

*Gestión de Proyecto*

El proyecto de gestión de BCP involucra a las áreas responsables de los procesos de soporte y a las áreas responsables de las operaciones.
Un proyecto de BCP incluye:

- Análisis de impacto y análisis de riesgos
- Desarrollo de estrategias y planes de prevención y recuperación

- Implantación de las medidas
- Evaluación y monitoreo

## 3.10.2.-Análisis del impacto de negocio (BIA)

El análisis de impacto de negocio debe ser realizado por cada una de los departamentos que realiza actividades esenciales de negocio. El análisis de impacto de negocio debe establecer las diversas pérdidas en caso de que se deje de dar servicio durante un período de tiempo determinado.

Las pérdidas pueden deberse a responsabilidades civiles, pérdida de negocio, deterioro de imagen, requerimientos legales, costes de recuperación, etc...

El resultado del impacto de negocio debe ser una función que a partir del tiempo sin capacidad de ejecutar las actividades esenciales indique las pérdidas que se sufrirían y un umbral de pérdidas aceptables que indicará el tiempo máximo que se puede soportar un fallo de servicio.

¿Cuánto perdería un negocio en una hora? ¿Cuánto tiempo esperará un cliente por su producto o servicio antes que se vaya a la competencia? ¿En qué días, semanas o meses está una empresa más vulnerable a la pérdida de ingresos en caso de algún paro? ¿Qué multas o penalidades puede incurrir? Esas son algunas de las preguntas para todos (Mandujano Manuel, 2005).

Basado en las respuestas se fórmulan las estrategias para luego decidir la inversión y llegar a un punto de equilibrio en donde el desembolso no sobrepase el riesgo de la pérdida: “Una cosa es asumir un riesgo conociéndolo y otra es asumir un riesgo con los ojos cerrados”, expresó la Directora, quien también agregó: “Todo hombre de empresa sabe cuáles son sus operaciones críticas de negocio; lo que no puede decir es cuánto puede perder en uno, dos o tres días si se caen esas operaciones; qué interdependencia hay entre esas operaciones sobre otros procesos no tan obvios y cómo la interrupción de las mismas afecta a sus clientes(Mandujano Manuel, 2005).

“Esas respuestas las entrega un análisis de impacto del negocio (*business impact analysis*) y es lo primero que debe hacerse” (Mandujano Manuel, 2005).

El BIA tiene como objetivo evaluar el riesgo soportado por la organización, teniendo en cuenta los problemas potenciales que puedan afectar a su operación, y consiste en cuatro tareas principales (Recuperación de desastres):

1. Selección de los procesos de negocio críticos (para los cuales se pretende establecer una solución de recuperación en caso de desastre) y su respectiva Arquitectura de TI de soporte.

2. Identificación de los niveles de servicio que necesitan ser garantizados para cada proceso (a través de la evaluación del coste de la interrupción de los servicios y de la reposición de la información).
3. Identificación de los desastres potenciales.
4. Evaluación del impacto provocado, en cada proceso, por los diferentes tipos de Desastre y su probabilidad de ocurrencia.
5. Definición de las medidas que precisan ser implantadas para reducir el riesgo (Datos, Servidores, Centros de procesamiento, Locales de trabajo y comunicaciones) en base a un análisis de coste/beneficio.

## 3.10.3.-Análisis de riesgos

El análisis de riesgo valora la posibilidad de que se produzca un daño que afecte a los activos de la empresa. En el contexto de un Plan de Continuidad de negocio, el Análisis de Riesgos debe valorar los elementos que soportan a los procesos esenciales y los diversos riesgos que les pueden afectar: intencionados, negligencias o eventos naturales.

Algunos otros tipos de análisis que también se pueden realizar son:

- análisis del entorno del tecnológico
- Análisis de escenarios

**Estrategias de Continuidad**

Una vez establecidos los impactos al negocio y el nivel de riesgo se deben plantear diversas estrategias de continuidad. Estas estrategias deben permitir ejecutar los servicios en el plazo previsto por el análisis de impacto de negocio y con un coste paralelo de acuerdo al análisis de riesgos.

Las estrategias de continuidad se fundamentan en la disponibilidad de sistemas de soporte de operaciones que no sean afectados por la contingencia. Estos sistemas de soporte incluyen sistemas informáticos en reserva, copia remota de los datos, oficinas preparadas para ser utilizadas y contratos de reposición de emergencia.

*Desarrollo de plan para el comité de crisis*

Una vez ocurre una contingencia se debe convocar un comité de crisis previamente creado a tal efecto. Una vez establecida la gravedad del incidente, el comité de crisis debe tomar el control y garantizar la ejecución de los planes de contingencia previstos.

El éxito de un comité de crisis reside en su capacidad de llevar a cabo el plan de contingencia y de tener definidas todas las tareas y responsables necesarios para ejecutar los procesos.

El comité de crisis debe constituirse en la referencia dentro de la organización para todas las tareas de contención, recuperación y vuelta a la normalidad.

*Política de comunicación*

En el caso de que la crisis se haga pública, es necesario disponer de una política de comunicación coherente y centralizada acerca del incidente, su impacto y la recuperación por parte de la organización.

En el impacto de una crisis la percepción externa juega un papel importante, por este motivo y a partir del plan de contingencias de la entidad debe informarse de manera clara, sin alarmismos y teniendo en cuenta las responsabilidades en que se puede incurrir.

La política de comunicación debe incluir a priori notas de prensa y comunicados tipo, y establecer los responsables de comunicación en caso de crisis.

*Coordinación Externa*

La coordinación externa con las fuerzas del orden, reguladores, compañías de seguros,
etc. debe ser fluida y clara. Para minimizar impacto legal y conseguir el máximo apoyo de las entidades externas se debe detallar a cada entidad el impacto del incidente, las medidas de recuperación y el soporte requerido para reanudar el funcionamiento.

## *Plan de Operaciones de Emergencia*

Una vez que se ha producido la contingencia los servicios esenciales se deben seguir prestando pero los procedimientos para ejecutarlos serán diferentes. Cada responsable de los procesos esenciales debe establecer los procedimientos para trabajar en caso de contingencia. Estos procedimientos deben estar diseñados y probados previamente.

Ejemplos de planes de operaciones de emergencia es la aceptación o el envío de pedidos aunque los sistemas de inventario no estén activos utilizando registros manuales, la posibilidad de permitir reintegros en oficinas hasta cierto importe en el caso que los sistemas centrales no estén disponibles, etc.

Un Business Continuity Plan puede incluir varios tipos de documentos con objetivos distintos:

## 3.10.4.-Plan de Contingencia:

Abarca un **Conjunto de procedimientos** a aplicar en el caso que ocurra un evento particular que pueda afectar a la organización.

El plan de contingencias es una estrategia constituida por un conjunto de recursos ideados con el propósito de servir de respaldo, contando con una organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios de negocio efectuados por una paralización total o parcial de la capacidad operativa de la empresa.

Tal estrategia, puntualizada en un manual, es resultado de todo un proceso de análisis y definiciones que dan lugar a las metodologías. A su vez las metodologías existentes versan sobre el proceso necesario para obtener dicho plan.

Es muy importante tener en cuenta que el concepto a considerar es " la continuidad en el negocio" ; estudiar todo lo que pueda en un momento dado paralizar la actividad y producir pérdidas. Todo lo que no considere estos criterios no podrá ser nunca un plan de contingencias.

En el mundo de los negocios, la tecnología del cómputo ha incrementado su campo de acción desde transacciones de contabilidad de tabulación histórica, hasta asimilaciones de tiempo real en el manejo de datos complejos analógicos y digitales, así como en la formulación y la ejecución de procesos en procedimientos de control y seguridad.

Las computadoras han adquirido la capacidad de asimilar consistentemente los datos, variables, soluciones de desarrollo, y aplicarlos a la multitud de problemas de negociación. En general, la mayoría de los procesos para la toma de decisiones y los sistemas de control que han sido institucionalizados en sistemas computacionales.

Para la mayoría de las organizaciones la supuesta dependencia de los sistemas de cómputo durante un período de recuperación de desastres es un mito propiciado por los siguientes factores:

- Ausencia en una conciencia centralizada y en la prioridad de los Programas de Educación para tener un análisis del impacto en los negocios.

- Fallas en la exploración de las alternativas Un proceso educativo y la exploración de alternativas viables con el personal adecuado es la clave para la efectividad de los planes de contingencia a un costo adecuado.

Los planes de recuperación de desastes y la planeación continua de negocios involucran grandes consideraciones de planeación.

Existen generalmente tres áreas de acción a la que están dirigidos:
ð Pérdida de la capacidad de comunicación, como: voz y datos.
ð Perdida de la capacidad de procesamiento.
ð Perdida del espacio principal de trabajo.

La responsabilidad de llevar a cabo esta planeación dentro de las áreas funcionales de una organización puede ser asumida por departamentos individuales, sin embargo la planeación de contingencia debe ser coordinada centralizadamente. De forma tal que las relaciones ínter departamentales, las dependencias de un sistema con otros, y la necesidad de reducir duplicación de tareas en algunos puntos de la planeación justifican la necesidad de coordinar los procesos durante la planeación de contingencias en la corporación-completa.

## 3.10.5.-Recuperación frente a Desastres (DRP, Disaster Recovery Plan):

Son Procedimientos a aplicar en el caso que ocurra un incidente de tal magnitud que afecte a la totalidad de los **sistemas informáticos** de una organización. Además establece la estrategia de recuperación de las aplicaciones críticas, i.e., aquellas aplicaciones que soportan los procesos críticos del negocio

Es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre en el área Informática, considerando como tal todas las áreas de los usuarios que procesan información por medio de la computadora (Plan de recuperación de desastres).

Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

La elaboración de los procedimientos que se determinen como adecuados para un caso de emergencia, deben ser planeados y probados fehacientemente.

Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo

haber procesos de verificación de su cumplimiento. En estos procedimientos estará involucrado todo el personal de la Institución.

Los procedimientos de planes de recuperación de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.

Las actividades a realizar en un Plan de Recuperación de Desastres se pueden clasificar en tres etapas:

Actividades Previas al Desastre.

Actividades Durante el Desastre.

Actividades Después del Desastre

### 3.10.6.-Plan de Continuidad de Operaciones –

Establece el plan de recuperación de los procesos de negocio, a veces incluyendo procesos manuales alternativos.

### 3.11.-Evaluación y monitoreo

Una de las pruebas para determinar en una organización si existe una adecuada Implantación de los BCP es comprobar si se ha realizado algún simulacro y si las actualizaciones de sistemas y procesos se ven reflejadas en él.

Para mantener la salud de un plan de continuidad implica verificarlo al menos anualmente e incluir en cada proceso una actualización de las medidas del plan de continuidad.

Es importante realizar ensayos del plan, esto puede ser planteando diferentes escenarios para saber si el plan puede responder en la manera que esperamos.

También es importante auditarlo, pues de esta manera podemos saber si estamos cumpliendo con los requisitos necesarios para poder contrarrestar los incidentes.

### 3.12.-Métricas, variables e indicadores.

En este proceso se pueden determina algunas métricas para ser monitoreadas y poder conocer a través de ellas el estado en que se encuentra el proceso.

haber procesos de verificación de su cumplimiento. En estos procedimientos estará involucrado todo el personal de la Institución.

Los procedimientos de planes de recuperación de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.

Las actividades a realizar en un Plan de Recuperación de Desastres se pueden clasificar en tres etapas:

Actividades Previas al Desastre.

Actividades Durante el Desastre.

Actividades Después del Desastre

### 3.10.6.-Plan de Continuidad de Operaciones –

Establece el plan de recuperación de los procesos de negocio, a veces incluyendo procesos manuales alternativos.

### 3.11.-Evaluación y monitoreo

Una de las pruebas para determinar en una organización si existe una adecuada Implantación de los BCP es comprobar si se ha realizado algún simulacro y si las actualizaciones de sistemas y procesos se ven reflejadas en él.

Para mantener la salud de un plan de continuidad implica verificarlo al menos anualmente e incluir en cada proceso una actualización de las medidas del plan de continuidad.

Es importante realizar ensayos del plan, esto puede ser planteando diferentes escenarios para saber si el plan puede responder en la manera que esperamos.

También es importante auditarlo, pues de esta manera podemos saber si estamos cumpliendo con los requisitos necesarios para poder contrarrestar los incidentes.

### 3.12.-Métricas, variables e indicadores.

En este proceso se pueden determina algunas métricas para ser monitoreadas y poder conocer a través de ellas el estado en que se encuentra el proceso.

haber procesos de verificación de su cumplimiento. En estos procedimientos estará involucrado todo el personal de la Institución.

Los procedimientos de planes de recuperación de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.

Las actividades a realizar en un Plan de Recuperación de Desastres se pueden clasificar en tres etapas:

Actividades Previas al Desastre.

Actividades Durante el Desastre.

Actividades Después del Desastre

### 3.10.6.-Plan de Continuidad de Operaciones –

Establece el plan de recuperación de los procesos de negocio, a veces incluyendo procesos manuales alternativos.

### 3.11.-Evaluación y monitoreo

Una de las pruebas para determinar en una organización si existe una adecuada Implantación de los BCP es comprobar si se ha realizado algún simulacro y si las actualizaciones de sistemas y procesos se ven reflejadas en él.

Para mantener la salud de un plan de continuidad implica verificarlo al menos anualmente e incluir en cada proceso una actualización de las medidas del plan de continuidad.

Es importante realizar ensayos del plan, esto puede ser planteando diferentes escenarios para saber si el plan puede responder en la manera que esperamos.

También es importante auditarlo, pues de esta manera podemos saber si estamos cumpliendo con los requisitos necesarios para poder contrarrestar los incidentes.

### 3.12.-Métricas, variables e indicadores.

En este proceso se pueden determina algunas métricas para ser monitoreadas y poder conocer a través de ellas el estado en que se encuentra el proceso.

Las variables obtenidas para el proceso de BCP se encuentran listadas a continuación.

Tabla 4.- Variables e indicadores del proceso de BCP

| Variables | Descripción. |
|---|---|
| **Xbcp1**<br>Frecuencia:<br>1 año | Número de total de aplicaciones críticas que requieren respaldo<br>Objetivo.- Determinar el número total de aplicaciones que requieren respaldo |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xbcp2**<br>Frecuencia:<br>1 año | Número total de aplicaciones críticas que son respaldados frecuentemente de acuerdo a la norma<br>Objetivo.- Ayudará a determinar el porcentaje de aplicaciones críticas que requieren respaldo |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xbcp3**<br>Frecuencia:<br>1 año | Número de total de sistemas de la organización<br>Objetivo.- Determinar el número total de sistemas de la organización |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xbcp4**<br>Frecuencia:<br>1 año | Número total de sistemas que cuentan con un plan de contingencia.<br>Objetivo.- Ayudará a determinar el % total de sistemas con un plan de contingencia |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xbcp5**<br>Frecuencia:<br>1 año | Número de total de sistemas de gestión de negocio que tienen planes de contingencia probados<br>Objetivo.- Ayudará a construir una métrica del % de planes de contingencias probados. |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xbcp6**<br>Frecuencia:<br>1 año | Número total de unidades organizacionales<br>Objetivo.- Determinar el número total de unidades organizacionales para obtener métricas |
| Fuente: Corporate information security working group | |
| **Xbcp7**<br>Frecuencia:<br>1 año | Número de total de unidades organizacionales que cuentan con un plan de continuidad<br>Objetivo.- Ayudará a obtener un a métrica del porcentaje de unidades organizacionales que cuentan con un plan |
| Fuente: Corporate information security working group | |

| | |
|---|---|
| **Xbcp8**<br>Frecuencia:<br>1 año | Número total de unidades organizacionales que cuentan con un plan de continuidad documentado.<br>Objetivo.- Ayudará a determinar una métrica del porcentaje de unidades organizacionales que cuentan con un BCP documentado |
| Fuente: Corporate information security working group | |
| **Xbcp9**<br>Frecuencia:<br>1 año | Número de total de planes de BCP de unidades de negocios que son auditados<br>Objetivo.- Ayudará a obtener un a métrica del % de BCP de unidades organizacionales que son auditados |
| Fuente: Corporate information security working group | |
| **Xbcp10**<br>Frecuencia:<br>1 año | Número total de planes de BCP de unidades de negocios que son actualizados<br>Objetivo.- Determinar una métrica del % de BCP de unidades organizacionales que son Actualizados |
| Fuente: Corporate information security working group | |

Algunas métricas (indicadores) que podemos obtener a partir de estas variables son las siguientes:

| Indicadores | Descripción. |
|---|---|
| INDbcp1 | Porcentaje de aplicaciones críticas que son respaldados frecuentemente.<br>Fórmula = Xbcp2*100/Xbcp1 |
| | |
| INDbcp2 | Porcentaje de sistemas que cuentan con un plan de contingencia Fórmula = Xbcp4*100/Xbcp3 |
| | |
| INDbcp3 | Porcentaje de planes de contingencias probados<br>Fórmula = Xbcp5*100/Xbcp3 |
| | |
| INDbcp4 | Porcentaje de unidades organizacionales que cuentan con un Plan de continuidad<br>Fórmula = Xbcp7*100/Xbcp6 |
| | |

| | |
|---|---|
| INDbcp5 | Porcentaje de unidades organizacionales con un BCP documentado.<br>Fórmula = Xbcp8*100/Xbcp6 |
| | |
| INDbcp6 | Porcentaje de BCP de unidades de negocios que son auditados<br>Fórmula = Xbcp9*100/Xbcp7 |
| | |
| INDbcp7 | Porcentaje de BCP de unidades de negocios que son actualizados.<br>Fórmula = Xbcp10*100/Xbcp7 |
| | |

## *Política de seguridad de información corporativa*

### 3.13.-Introducción

La falta de políticas y procedimientos en seguridad es uno de los problemas más graves que confrontan las empresas hoy día en lo que se refiere a la protección de sus activos de información frente a peligros externos e internos (Víctor Cappuccio, 2002).

Las políticas de seguridad son esencialmente orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base de un plan maestro para la implantación efectiva de medidas de protección tales como: identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos (Víctor Cappuccio, 2002).

Cualquier política ha de contemplar seis elementos claves en la seguridad de un sistema informático.

- Disponibilidad
  Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesitan, especialmente la información crítica.
- Utilidad
  Los recursos del sistema y la información manejada en el mismo ha de ser útil para alguna función.
- Integridad
  La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
- Autenticidad
  El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.
- Confidencialidad
  La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.
- Posesión
  Los propietarios de un sistema han de ser capaces de controlarlo en todo momento; perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios(Antonio Villalón Huerta Antonio, 2002)

### 3.14.- Definición Política de seguridad.

Por política de seguridad se entiende aquel documento en el que se identifican pormenorizadamente las necesidades específicas y los procedimientos a seguir en materia de seguridad, teniendo siempre en cuenta las condiciones y

## *Política de seguridad de información corporativa*

### 3.13.-Introducción

La falta de políticas y procedimientos en seguridad es uno de los problemas más graves que confrontan las empresas hoy día en lo que se refiere a la protección de sus activos de información frente a peligros externos e internos (Víctor Cappuccio, 2002).

Las políticas de seguridad son esencialmente orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base de un plan maestro para la implantación efectiva de medidas de protección tales como: identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos (Víctor Cappuccio, 2002).

Cualquier política ha de contemplar seis elementos claves en la seguridad de un sistema informático.

- Disponibilidad
  Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesitan, especialmente la información crítica.
- Utilidad
  Los recursos del sistema y la información manejada en el mismo ha de ser útil para alguna función.
- Integridad
  La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
- Autenticidad
  El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.
- Confidencialidad
  La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.
- Posesión
  Los propietarios de un sistema han de ser capaces de controlarlo en todo momento; perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios(Antonio Villalón Huerta Antonio, 2002)

### 3.14.- Definición Política de seguridad.

Por política de seguridad se entiende aquel documento en el que se identifican pormenorizadamente las necesidades específicas y los procedimientos a seguir en materia de seguridad, teniendo siempre en cuenta las condiciones y

circunstancias propias de cada organización. En dicho documento tiene que tener cabida toda aquella información que identifique claramente los puntos que se han de proteger, estableciendo un riguroso orden de prioridad en función de su mayor o menor impacto en la continuidad y disponibilidad de los servicios que se ofrezca al usuario.

Con este proceder se reduce al máximo el posible error de proteger áreas de nuestra infraestructura tecnológica intrascendentes de cara a la productividad del mismo, mientras se dejan al descubierto otras que resultan mucho más críticas para la buena marcha del negocio. Además, se ha de asegurar la Confidencialidad de los datos, la integridad de la red y la autenticidad de los usuarios con derechos de acceso.

Teniendo en mente todas estas facetas de actuación, se podrá determinar la mejor estrategia de seguridad para garantizar un lógico nivel de protección de nuestro negocio. Pero no basta con crear una política de seguridad, sino que hay que comunicarla bien a los miembros del grupo, con el fi n de evitar en lo posible los inconvenientes que estos puedan causar (3com).

Si bien las políticas varían considerablemente según el tipo de organización de que se trate, en general incluyen declaraciones generales sobre metas, objetivos, comportamiento y responsabilidades de los empleados en relación a las violaciones de seguridad. A menudo las políticas van acompañadas de instrucciones, normas, estándares y procedimientos (ilustrados.com).

Una política de seguridad explica con documentación el por qué una organización protege su información.

Los estándares de la organización explican con documentación lo qué la organización quiere hacer para implementar y administrar la seguridad de su información.

Los procedimientos explican con documentación exactamente cómo la organización obtendrá los requerimientos ordenados por estándares y políticas de nivel superior

Para una mejor comprensión se describe a continuación la diferencia entre cada una de estas definiciones.

**Documento de la política de seguridad**

Es importante anotar que la política de seguridad de la información de una organización es un simple documento que articula la filosofía, los requerimientos reglamentarios y las creencias que la organización tiene en relación con la

protección a los recursos de la información. Esta política explica con documentación el enfoque del medio ambiente, del personal y de los procesos en donde la aplica, así como las consecuencias de su incumplimiento. La Política de Seguridad de la Información es parte de un conjunto de políticas que generalmente cumplen las organizaciones. Otras políticas solucionan áreas críticas como los recursos humanos, las instalaciones y las finanzas. Estas otras políticas deben ser complementadas y respaldadas con La Política de Seguridad de la Información.

**Estándares**

Los estándares de seguridad de la información constan de documentos múltiples que se aplican a todas las áreas de la empresa que utilizan la información. Estos estándares abarcan controles de seguridad físicos, administrativos y lógicos (técnicos) que están diseñados para proteger la información. Uno de los documentos de estándares define el contenido y presentación de toda la documentación de seguridad de la compañía de manera que muchas organizaciones contarán con docenas de documentos de los estándares para la seguridad de la información.

**Procedimientos**

Los procedimientos de seguridad de la información establecen de manera detallada las operaciones que necesitan realizarse para satisfacer los requerimientos especificados en el Estándar que se aplica a una actividad determinada, proceso de seguridad o protección a un recurso de la información (Symantec, 2004).

**Guía**

Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo (Universidad nacional de Colombia,2003).

Las políticas son obligatorias, mientras que las recomendaciones o directrices son más bien opcionales. De hecho, las declaraciones de políticas de seguridad pueden transformarse fácilmente en recomendaciones reemplazando la palabra "debe" con la palabra "debería"( Víctor Cappuccio, 2002).

Por otro lado las políticas son de jerarquía superior a las normas, estándares y procedimientos que también requieren ser acatados. Las políticas consisten de declaraciones genéricas, mientras las normas hacen referencia específica a tecnologías, metodologías, procedimientos de implementación y otros aspectos

en detalle. Además las políticas deberían durar durante muchos años, mientras que las normas y procedimientos duran menos tiempo (Víctor Cappuccio, 2002).

Las normas y procedimientos necesitan ser actualizadas más a menudo que las políticas porque hoy día cambian muy rápidamente las tecnologías informáticas, las estructuras organizativas, los procesos de negocios y los procedimientos. Por ejemplo, una norma de seguridad de cifrado podría especificar el uso del estándar DES (Data Encryption Standard). Esta norma probablemente deberá será revisada o reemplazada en los próximos años (Víctor Cappuccio, 2002).

## 3.15.- Elementos de una política de seguridad.

Como hablamos en la sección anterior, una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere una disposición de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las PSI deben considerar entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que él o ella tiene acceso.

Las PSI deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones, transmitir por qué son importantes éstos u otros recursos o servicios.

De igual forma, las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otro lado, la política de debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. No debe

en detalle. Además las políticas deberían durar durante muchos años, mientras que las normas y procedimientos duran menos tiempo (Víctor Cappuccio, 2002).

Las normas y procedimientos necesitan ser actualizadas más a menudo que las políticas porque hoy día cambian muy rápidamente las tecnologías informáticas, las estructuras organizativas, los procesos de negocios y los procedimientos. Por ejemplo, una norma de seguridad de cifrado podría especificar el uso del estándar DES (Data Encryption Standard). Esta norma probablemente deberá será revisada o reemplazada en los próximos años (Víctor Cappuccio, 2002).

## 3.15.- Elementos de una política de seguridad.

Como hablamos en la sección anterior, una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere una disposición de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las PSI deben considerar entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que él o ella tiene acceso.

Las PSI deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones, transmitir por qué son importantes éstos u otros recursos o servicios.

De igual forma, las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otro lado, la política de debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. No debe

especificar con exactitud que pasará cuando algo suceda; no es una sentencia obligatoria de la ley.

Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios entre otros.

a continuación se muestra un ejemplo de desarrollo de una política de seguridad.

1.- introducción
- 1.1.1 Información general.
- 1.1.2 Objetivos
- 1.2.- Responsabilidades de la estructura organizacional.
- 1.2.2.- Estándares de seguridad.

2.- Servicios de dominio.
3.- Sistemas de E-mail
4.- Servicios Web
5.- Centro de datos
6.- LAN/WAN
7.- Sistemas Desktop
8.- Sistemas de telecomunicaciones
9.- Servicios estratégicos
10.- Sistemas de herencia
11.- Seguridad en Procedimientos y servicios.
12.- Dirección de incidente de seguridad
13.- Actividades en curso.
14.- Contactos, lista de mail, y otros recursos.
15.- Referencias.

## 3.16.-Etapas del en el diseño e implementación de la política.

Existen 4 etapas en el desarrollo de una política. Las cuales se describen a continuación.

**Fase de desarrollo.-** durante esta fase la política es creada, revisada y aprobada.
**Fase de implementación.-** En esta fase la política es comunicada y acatada(o no cumplida por alguna excepción).
**Fase de fase de mantenimiento.-**Los usuarios deben ser concientes de la importancia de la política, su cumplimiento debe ser monitoreado, se debe garantizar su cumplimiento y se le debe dar mantenimiento (actualizarla).

especificar con exactitud que pasará cuando algo suceda; no es una sentencia obligatoria de la ley.

Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios entre otros.

a continuación se muestra un ejemplo de desarrollo de una política de seguridad.

1.- introducción
- 1.1.1 Información general.
- 1.1.2 Objetivos
- 1.2.- Responsabilidades de la estructura organizacional.
- 1.2.2.- Estándares de seguridad.

2.- Servicios de dominio.
3.- Sistemas de E-mail
4.- Servicios Web
5.- Centro de datos
6.- LAN/WAN
7.- Sistemas Desktop
8.- Sistemas de telecomunicaciones
9.- Servicios estratégicos
10.- Sistemas de herencia
11.- Seguridad en Procedimientos y servicios.
12.- Dirección de incidente de seguridad
13.- Actividades en curso.
14.- Contactos, lista de mail, y otros recursos.
15.- Referencias.

## 3.16.-Etapas del en el diseño e implementación de la política.

Existen 4 etapas en el desarrollo de una política. Las cuales se describen a continuación.

**Fase de desarrollo.-** durante esta fase la política es creada, revisada y aprobada.
**Fase de implementación.-** En esta fase la política es comunicada y acatada(o no cumplida por alguna excepción).
**Fase de fase de mantenimiento.-**Los usuarios deben ser concientes de la importancia de la política, su cumplimiento debe ser monitoreado, se debe garantizar su cumplimiento y se le debe dar mantenimiento (actualizarla).

**Fase de eliminación.-** la política se retira cuando no se requiere más.

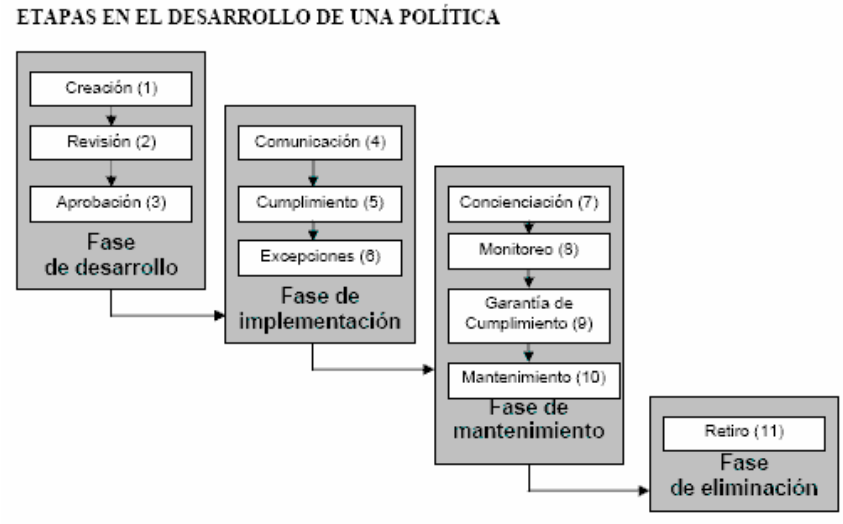



Figura 4.- Etapas de implementación de políticas.

## 3.17.- Parámetros importantes en una política de seguridad.

- Es importante que la alta dirección apoye y participe en todo el proceso de elaboración de políticas, pues de ellos depende en gran manera el éxito que las políticas puedan tener dentro de la empresa.
- Considere efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá afinar las PSI de su organización.
- Involucre a los áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.
- Comunique a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Recuerde que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los interesados en salvaguardar los activos críticos de la funcionalidad de su área u organización.
- Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas
- Un consejo más, no dé por hecho algo que es obvio. Haga explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI trazadas. (jeimy J. Cano)

**Fase de eliminación.-** la política se retira cuando no se requiere más.

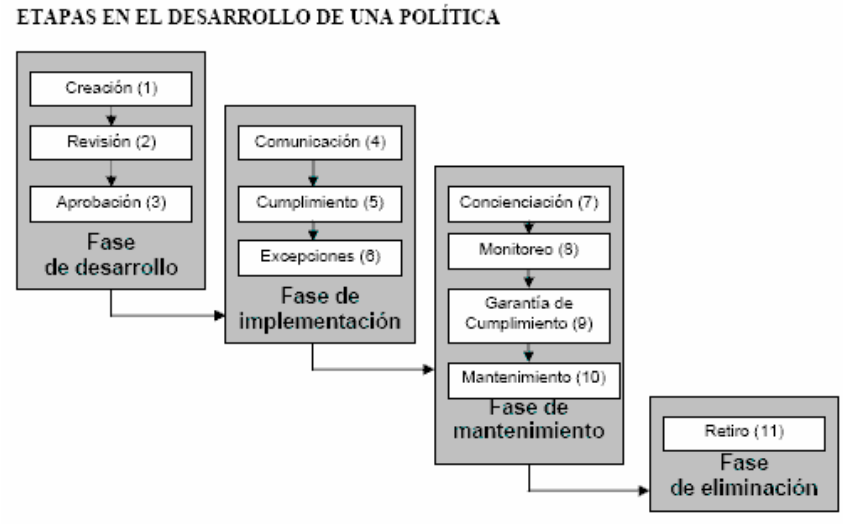



Figura 4.- Etapas de implementación de políticas.

## 3.17.- Parámetros importantes en una política de seguridad.

- Es importante que la alta dirección apoye y participe en todo el proceso de elaboración de políticas, pues de ellos depende en gran manera el éxito que las políticas puedan tener dentro de la empresa.
- Considere efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá afinar las PSI de su organización.
- Involucre a los áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.
- Comunique a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Recuerde que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los interesados en salvaguardar los activos críticos de la funcionalidad de su área u organización.
- Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas
- Un consejo más, no dé por hecho algo que es obvio. Haga explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI trazadas. (jeimy J. Cano)

## 3.18.-Problemas para implantar una política de seguridad.

Muchas veces las organizaciones realizan grandes esfuerzos para definir sus directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, con relativo éxito. Según algunos estudios [5] resulta una labor ardua el convencer a los altos ejecutivos de la necesidad de buenas políticas y prácticas de seguridad informática.

Muchos de los inconvenientes se inician por los tecnicismos informáticos y la falta de una estrategia de mercadeo de los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: "más dinero para los juguetes de los ingenieros". Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad, que en muchos de los casos lleva a comprometer su información sensitiva y por ende su imagen corporativa.

Ante esta encrucijada, los encargados de la seguridad deben asegurarse de que las personas relevantes entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

En particular, la gente debe saber las consecuencias de sus decisiones, incluyendo lo mejor y lo peor que podría ocurrir. Una buena intrusión o una travesura podrían convertir a las personas que no entendieron, en blanco de las políticas o en señuelos de los verdaderos vándalos.

Luego, para que las PSI logren abrirse espacio al interior de una organización deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía. De igual forma, las PSI deben ir acompañadas de una visión de negocio que promueva actividades que involucren a las personas en su diario hacer, donde se identifiquen las necesidades y acciones que materializan las políticas.

En este contexto, el entender la organización, sus elementos culturales y comportamientos nos deben llevar a reconocer las pautas de seguridad necesaria y suficiente que aseguren confiabilidad en las operaciones y funcionalidad de la compañía (jeimy J. Cano).

## 3.19.- Métricas Variables e indicadores.

Las variables obtenidas para el proceso de política corporativa se encuentran descritas a continuación:

Tabla 5.- Variables e indicadores del proceso de política

## 3.18.-Problemas para implantar una política de seguridad.

Muchas veces las organizaciones realizan grandes esfuerzos para definir sus directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, con relativo éxito. Según algunos estudios [5] resulta una labor ardua el convencer a los altos ejecutivos de la necesidad de buenas políticas y prácticas de seguridad informática.

Muchos de los inconvenientes se inician por los tecnicismos informáticos y la falta de una estrategia de mercadeo de los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: "más dinero para los juguetes de los ingenieros". Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad, que en muchos de los casos lleva a comprometer su información sensitiva y por ende su imagen corporativa.

Ante esta encrucijada, los encargados de la seguridad deben asegurarse de que las personas relevantes entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

En particular, la gente debe saber las consecuencias de sus decisiones, incluyendo lo mejor y lo peor que podría ocurrir. Una buena intrusión o una travesura podrían convertir a las personas que no entendieron, en blanco de las políticas o en señuelos de los verdaderos vándalos.

Luego, para que las PSI logren abrirse espacio al interior de una organización deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía. De igual forma, las PSI deben ir acompañadas de una visión de negocio que promueva actividades que involucren a las personas en su diario hacer, donde se identifiquen las necesidades y acciones que materializan las políticas.

En este contexto, el entender la organización, sus elementos culturales y comportamientos nos deben llevar a reconocer las pautas de seguridad necesaria y suficiente que aseguren confiabilidad en las operaciones y funcionalidad de la compañía (jeimy J. Cano).

## 3.19.- Métricas Variables e indicadores.

Las variables obtenidas para el proceso de política corporativa se encuentran descritas a continuación:

Tabla 5.- Variables e indicadores del proceso de política

| Variables | Descripción. |
|---|---|
| **Xpol1**<br>Frecuencia:<br>6 meses | Número de total de sistemas con passwords<br>Objetivo.- Determinar el número total de sistemas con passwords de la organización para elaborar métricas |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xpol2** Frecuencia:<br>6 meses | Número total de sistemas que cuentan con política de password<br>Objetivo.- Ayudará a determinar el % de sistemas que cuentan con política de password |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xpol3**<br>Frecuencia:<br>6 meses | Número de total de websites con los que cuenta la organización<br>Objetivo.- Determinar el número total de websites con los que cuenta la organización para poder obtener métricas |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xpol4** Frecuencia:<br>6 meses | Número total de websites que cuentan con política de seguridad incorporada<br>Objetivo.- Ayudará a determinar el % de websites que cuentan con política de seguridad incorporada |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xpol5**<br>Frecuencia:<br>6 meses | Número de proveedores o de outsourcing con los que tiene relación la empresa<br>Objetivo.- Determinar el número total de proveedores o de outsourcing para poder establecer métricas |
| Fuente: Corporate information security working group | |
| **Xpol6**<br>Frecuencia:<br>6 meses | Número de proveedores o de outsourcing con los que se ha establecido una políticas de seguridad para el intercambio de información<br>Objetivo.- Determinar el % de proveedores o outsourcing con los que se han establecido políticas de seguridad. |
| Fuente: Corporate information security working group | |
| **Xpol7** Frecuencia:<br>6 meses | Número de políticas corporativas totales que existen en la organización<br>Objetivo.- Determinar el número total de políticas corporativas que existen en una organización |
| Fuente: Corporate information security working group | |
| **Xpol8**<br>Frecuencia:<br>6 meses | Número de políticas especificas que han sido violadas por los usuarios<br>Objetivo.- Ayudará a determinar el % de políticas que han sido violadas |
| Fuente: Corporate information security working group | |
| **Xpol9** Frecuencia:<br>6 meses | Número de políticas que son actualizadas<br>Objetivo.- Determinar una métrica del % de políticas Actualizadas |

| | |
|---|---|
| Fuente: Personal | |
| **Xpol10**<br>Frecuencia:<br>1 año | Número de políticas que son auditadas<br>Objetivo.- Determinar una métrica del % de políticas auditadas |
| Fuente: Personal | |
| **Xpol11**<br>Frecuencia:<br>1 año | Número de políticas nuevas creadas<br>Objetivo.- Determinar el número de nuevas políticas creadas en un período de tiempo determinado |
| Fuente: Corporate information security working group | |
| **Xpol12**<br>Frecuencia:<br>1 año | Número de aplicaciones que cuentan con procedimiento de respaldo en la organización<br>Objetivo.- Determina el número total de aplicaciones con procedimiento de respaldo con que cuenta la empresa |
| Fuente: Corporate information security working group | |
| **Xpol13**<br>Frecuencia:<br>1 año | Número de aplicaciones cuyo respaldos se realizan de acuerdo a la política de respaldo<br>Objetivo.- Determinar una métrica del % de aplicaciones con procedimientos de respaldos que se apegan a la política. |
| Fuente: Corporate information security working group | |

Algunas métricas que podemos construir a partir de estas variables se listan a continuación.

| Indicadores | Descripción. |
|---|---|
| INDpol1 | Porcentaje de sistemas con política de password<br>Fórmula = Xpol2*100/Xpol1 |
| | |
| INDpol2 | Porcentaje de websites que cuentan con política de seguridad<br>Frecuencia = Xpol4*100/Xpol3 |
| | |
| INDpol3 | Porcentaje de proveedores o de outsourcing con los que se han desarrollado políticas de seguridad<br>Fórmula = Xpol6*100/Xpol5 |
| | |
| INDpol4 | Porcentaje de políticas especificas que han sido violadas por los usuarios<br>Fórmula = Xpol8*100/Xpol7 |

| | |
|---|---|
| | |
| INDpol5 | Porcentaje de políticas actualizadas<br>Fórmula = Xpol9*100/Xpol7 |
| | |
| INDpol6 | Porcentaje de políticas que son auditadas<br>Fórmula = Xpol10*100/Xpol7 |
| | |
| INDpol7 | Número de políticas nuevas creadas periódicamente<br>Fórmula = Xpol11 |
| | |
| INDpol8 | Porcentaje de aplicaciones con procedimiento de respaldo que se apega a la política de respaldo<br>Fórmula = Xpol13*100/Xpol11 |
| | |

## *Proceso de respuesta a incidentes.*

### 3.20.-Introducción

Un Equipo de Respuesta a Incidentes de Seguridad (CSIRT) es una organización que es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad. Sus servicios son generalmente prestados para un área de cobertura definida que podría ser una entidad relacionada u organización de la cual dependen, una corporación, una organización de gobierno o educativa; una región o país, una red de investigación; o un servicio pago para un cliente.

Un CSIRT puede ser un equipo formalizado o un equipo ad hoc. Un equipo formalizado realiza un trabajo de respuesta a incidentes como su función principal. A un equipo ad hoc se lo convoca durante un incidente de seguridad que esté ocurriendo en ese momento o para responder a un incidente cuando surge la necesidad.

Aún la mejor infraestructura de seguridad de la información no puede garantizar que las intrusiones y otros actos maliciosos no ocurran. Cuando ocurren incidentes de seguridad, será crítico que una organización tenga el modo efectivo de responder.

La velocidad con la cual una organización puede reconocer, analizar y responder a un incidente limitará el daño y bajará el costo de recuperación. Un CSIRT puede estar in-situ y ser capaz de conducir una respuesta rápida para contener un incidente de seguridad y recuperarse del mismo. Los CSIRTs pueden también estar familiarizados con los sistemas comprometidos y por lo tanto estar disponibles más rápidamente para coordinar la recuperación y proponer las estrategias de mitigación y respuesta.

Sus relaciones con otros CSIRTs y organizaciones de seguridad pueden facilitar la tarea de compartir estrategias de respuesta y alertar tempranamente acerca de los problemas potenciales. En forma proactiva, los CSIRTs pueden trabajar con otras áreas de la organización para asegurar que los nuevos sistemas sean desarrollados y desplegados con “el concepto de seguridad en mente” y de acuerdo con las políticas de seguridad de cualquiera fuere el sitio. Pueden ayudar a identificar las áreas vulnerables de la organización y en algunos casos realizar evaluaciones de vulnerabilidad y detección de incidentes.

Pueden centralizar la atención en la seguridad y hacer capacitación en concientización sobre seguridad informática para el área de cobertura. Los

CSIRTs también pueden ofrecer experiencia para hacer análisis preventivos y de predicción para ayudar a mitigar amenazas futuras (Arcert, 2004).

### 3.21.-Pasos para el desarrollo de un CSIRT

Aunque los CSIRTs diferirán en cómo operarán dependiendo del personal disponible, la experiencia, los recursos de presupuesto y las circunstancias únicas de cada organización, hay algunas prácticas básicas que se aplican para todos los CSIRTs. Trataremos algunas de estas prácticas en cuanto a lo que se relaciona con la creación de un CSIRT. (Para más información sobre qué es un CSIRT, ver CSIRT FAQ .) Aunque estas acciones están presentadas como pasos, el proceso es no secuencial; muchos pasos pueden ocurrir paralelamente.

## 3.21.1.-Obtener apoyo por parte de la gerencia.

Nuestra experiencia muestra que sin la aprobación y el apoyo gerencial, crear una capacidad efectiva de respuesta a incidentes puede ser extremadamente difícil y problemático. Este apoyo debe ser mostrado en diferentes formas, incluyendo la provisión de recursos, fondos, y tiempo a la persona o grupo de personas que actuarán como equipo de proyecto para la implementación del CSIRT. Esto también incluye gerentes ejecutivos y de negocios o de departamento y su personal, que comprometan su tiempo para participar en este proceso de planificación; su aporte es esencial durante los trabajos de diseño.

Es importante obtener las expectativas y percepciones de la gerencia acerca de la función y responsabilidades del CSIRT. Sin esta información, se puede construir un equipo cuyos servicios y autoridad no sean comprendidos o usados apropiadamente por el resto de la organización.

Además de obtener el apoyo gerencial para el proceso de planificación e implementación, es igualmente importante obtener el compromiso gerencial para sostener las operaciones y autoridad del CSIRT a largo plazo. Una vez que el equipo esté establecido ¿cómo se lo mantiene y expande con presupuesto, personal y recursos de equipamiento? ¿El rol y autoridad del CSIRT seguirán estando apoyados por la gerencia para todas las áreas de coberturas u organizaciones de la cual dependen? Sin este apoyo continuo el éxito de los CSIRT's a largo plazo estará en riesgo (ArcertII, 2004).

## 3.21.2.-Recabar información importante.

Recabar información para determinar la respuesta al incidente y las necesidades de servicio que tiene la organización. Dar una mirada a los tipos de actividad de incidentes que están siendo informados dentro de su institución. Esto ayuda a determinar no sólo qué tipo de servicio ofrecer sino también los tipos de habilidades y experiencia que necesitará el personal del CSIRT. Por ejemplo, si

su organización ha sido víctima de un virus de computadora o de la actividad de un gusano, usted necesitará un equipo con experiencia en virus para manejar la respuesta. También necesitará procedimientos de escaneo, eliminación y recuperación del virus, junto con las herramientas antivirus apropiadas. Usted puede requerir gente con buena capacitación y habilidades en documentación para ayudar a desarrollar programas de concientización del usuario como un paso proactivo para el tratamiento de la actividad del virus.

Identificar qué información necesita para saber cómo planear e implementar el CSIRT. Determinar quién tiene esa información y cómo obtener mejor esa información, ya fuere a través de discusiones generales o entrevistas o haciéndolos parte del proyecto.

Reunirse con los interesados claves para discutir no sólo sus necesidades de respuesta a incidentes, sino para lograr un consenso inicial sobre las expectativas, dirección estratégica, definiciones y responsabilidades del CSIRT. Su definición sobre qué es y hace un CSIRT puede ser muy diferente a la definición de su gerente o la definición de otra parte de su organización. ] Aproveche estas discusiones con los interesados o involucrados en el proyecto para delinear e identificar cómo cada grupo necesitará interactuar con el CSIRT. Los interesados o involucrados podrían incluir pero no están limitados a:

- **Gerentes de la empresa**.

  Ellos necesitan comprender qué es el CSIRT y cómo pueden ayudar a sostener los procesos de su negocio. Se deben hacer acuerdos referentes a la autoridad del CSIRT sobre los sistemas de la empresa y quién tomará las decisiones si los sistemas críticos de la empresa deben ser desconectados de la red o cerrados.

- **Representantes de Tecnología de la Información (IT)**.

  ¿Cómo interactúa el personal de IT y del CSIRT? ¿Qué acciones son tomadas por el personal de IT y qué acciones son tomadas por los miembros del CSIRT durante las operaciones de respuesta? ¿El CSIRT tendrá acceso a la red y los documentos del sistema con fines de análisis? ¿Podrá el CSIRT hacer recomendaciones para mejorar la seguridad de la infraestructura de la organización?

- **Representantes del departamento legal**.

  ¿Cuándo y cómo está involucrado el departamento legal en las tareas de respuesta a incidentes? También se puede requerir personal del área legal para revisar los acuerdos de no revelación de información, hacer la redacción apropiada para contactar otros sitios y organizaciones y para determinar la responsabilidad del sitio para los incidentes de seguridad.

- **Representantes de recursos humanos**.

Pueden ayudar a desarrollar las descripciones de tarea para contratar al personal de CSIRT, y desarrollar las políticas y procedimientos para remover a los empleados internos que se los encuentre comprometidos en una actividad informática no autorizada o ilegal.

- **Representantes de relaciones públicas**.

Deben estar preparados para manejar cualquier cuestionario de los medios y ayudar a desarrollar políticas y prácticas para revelación de información.

- **Cualquier grupo de seguridad existente, incluyendo seguridad física**.

El CSIRT necesitará intercambiar información acerca de incidentes informáticos con estos grupos y pueden compartir la responsabilidad con ellos para resolver temas que involucren robo de computadoras o datos.

- **Especialistas en auditoria y manejo de riesgos**.

Pueden ayudar a desarrollar métricas de amenaza y evaluaciones de vulnerabilidad, y al mismo tiempo alentar las mejores prácticas de seguridad en toda el área de cobertura u organización.

- **Representantes generales del área de cobertura**.

que pueden ofrecer una visión de sus necesidades y requerimientos.

Los interesados o involucrados también deberían incluir a cualquier persona que participará en el manejo del incidente o en el proceso de notificación. Piense quién necesitará ser notificado durante los diferentes tipos de incidentes. ¿Hay gente en otras partes de la organización o área de cobertura que puedan suministrar información o datos al CSIRT o con quienes el CSIRT necesitará compartir u obtener información? Éstos pueden incluir otras partes de IT o departamentos de seguridad, incluyendo grupos haciendo evaluaciones de vulnerabilidad, detección de intrusiones, o monitoreo de la red. Saber qué es lo que el CSIRT necesitará hacer puede ayudar a identificar la gente apropiada que deberá participar para desarrollar los procedimientos.

Encontrar si alguien más está actualmente realizando cualquiera de los servicios que el CSIRT pueda estar buscando ofrecer. Determinar si esos servicios deberán permanecer con el grupo actual o trasladarse al CSIRT durante un período de tiempo acordado. El tratamiento de estos tipos de temas en las etapas de planificación puede ayudar a identificar qué

responsabilidades deberán ser delineadas y qué información se necesitará reunir.

También puede haber algunos recursos disponibles para evaluar que ayudarán en la tarea de reunión información. Estos pueden incluir:

- Organigrama de la empresa y las funciones específicas del negocio
- Topologías para los sistemas y redes de la organización o el área de cobertura
- Sistema crítico e inventarios de activos
- Planes existentes de recuperación de desastres y continuidad del negocio
- Instrucciones existentes para notificar a la organización sobre el incumplimiento de una seguridad física
- Cualquier plan existente de respuesta a un incidente
- Cualquier reglamentación de la organización o institución
- Cualquier política o procedimiento de seguridad existente

Evaluar estos documentos tiene un doble fin: primeramente, identificar los involucrados existentes, los recursos y los propietarios del sistema; y segundo, proporcionar una visión general de las políticas existentes a las cuales se debe adherir el CSIRT. Como beneficio extra, estos documentos pueden contener un texto que puede ser adaptado cuando se desarrollen las políticas, procedimientos o documentación del CSIRT. También pueden incluir listas de notificación generales de los representantes de la organización que deben ser contactados durante las emergencias. Dichas listas pueden ser adaptadas para el trabajo y procesos del CSIRT.

Además, investigar qué están haciendo las organizaciones similares para proporcionar servicios de manejo de incidentes o para organizar un CSIRT. Si usted tiene contacto con estas organizaciones, vea si puede hablar con ellos acerca de cómo se formó el equipo. Preste atención a los sitios web de otros CSIRT y verifique sus misiones, estatutos, esquema de financiación y listado de servicios. Esto puede darle ideas para organizar su equipo. Revise otros libros o publicaciones sobre manejo de incidentes o CSIRTs. En la página web CERT CSIRT Development web page se puede encontrar una lista inicial de recursos.

Asistir a cursos o conferencias que tengan sesiones para desarrollar estrategias de respuesta a incidentes o para crear CSIRTs. Estos ámbitos ofrecen la oportunidad de intercambiar ideas e interactuar con otros en el campo de respuesta a incidentes. Un buen lugar para comenzar puede ser asistir a la conferencia anual FIRST conference(ArcertII, 2004)

## 3.21.3.-Comenzar la implantación del SCIRT.

El objetivo principal de SCIRT es prevenir y responder a incidentes, para comenzar la implantación primeramente necesitamos:

- Contratar y capacitar al personal inicial del CSIRT.
- Comprar el equipamiento y construir cualquier infraestructura de red necesaria para apoyar al equipo.
- Desarrollar el conjunto de políticas y procedimientos iniciales del CSIRT para respaldar sus servicios.
- Definir las especificaciones para, y construir, su sistema de rastreo de incidentes.
- Desarrollar las instrucciones y formularios para la información de incidentes para su área de cobertura.

Para la implantación también es importante identificar los sistemas que serán elegidos como blancos por los atacantes.

Un recurso importante que necesitará para su área de cobertura son los lineamientos e instrucciones para el informe de incidentes. Estas instrucciones definen cómo un distrito interactúa con su CSIRT, qué constituye un incidente, qué tipos de incidentes informar, quién debería informar un incidente, por qué un incidente debería ser informado, el proceso para informar un incidente y el proceso para responder a un incidente. Las instrucciones deben ser claras y de fácil comprensión por parte del distrito que está siendo atendido servido.

El proceso para informar un incidente incluye una descripción detallada de los mecanismos para presentar los informes: teléfono, correo electrónico, formulario web, o algún otro mecanismo. También debería incluir detalles acerca de qué tipo de información debería ser incluida en el informe.

El proceso para responder a un incidente describe cómo el CSIRT prioriza y maneja los informes recibidos. Esto incluye cómo la persona que informa un incidente es notificada de su resolución, cualquier margen de tiempo que deba seguirse, y cualquier otra notificación que hubiere.

Para ver un ejemplo de lineamiento e instrucciones para informar incidentes, abra CERT/CC Incident Reporting Guidelines .

## 3.21.4.-Evaluar la efectividad del SCIRT.

Una vez que el CSIRT haya estado funcionando durante algún tiempo, la gerencia querrá determinar la efectividad del equipo y usar los resultados de una evaluación para mejorar los procesos del CSIRT y asegurar que el equipo está

cumpliendo con las necesidades del área de cobertura. El CSIRT, en conjunto con la gerencia y el área de cobertura, necesitará desarrollar un mecanismo para realizar la evaluación.

La información sobre la efectividad puede ser reunida a través de una variedad de mecanismos de recepción de opiniones, que incluyen

- punto de referencia para comparación (Benchmark) con respecto a otros CSIRTs
- discusiones generales con representantes del área de cobertura
- encuestas de evaluación distribuidas a los miembros del área de cobertura periódicamente
- creación de un grupo de criterios o parámetros de calidad para que luego utilice un auditor o grupo externo para evaluar el equipo

## 3.22.-Tipos de incidentes

Algunos tipos de incidentes a los sistemas pueden ser:

1) Violación de una política.
2) Acceso no autorizado
3) Negación de recursos.
4) Uso no autorizado
5) Cambios sin el consentimiento, conocimiento y autorización de los propietarios.

A más nivel de detalle pueden ser:

1) Denial of services
2) Email Spoofing
3) Espianoge
4) Fraud
5) Inappropiate Use.
6) Malicious Code (Including Viruses).
7) Probes and Network Mapping.
8) Unauthorised Acces
9) Unlicenced/Pirate Software.
10) Warnings and Hoaxes.

## 3.23.-Como dar respuesta a los incidentes.

Toda red será antes o después víctima de un incidente relacionado con la seguridad de los equipos. Los administradores de sistemas necesitan estar preparados para enfrentarse a incidentes relacionados con la seguridad y responder de una manera rápida con el fin de minimizar y reparar los daños.

### Preparación para afrontar un incidente relacionado con la seguridad

Estar preparado para enfrentarse a un incidente relacionado con la seguridad es esencial para resolver rápidamente un suceso de intrusión cuando éste se produzca.

1. Recibir formación sobre seguridad

2. Realizar un inventario de los sistemas para su protección

3. Proteger los sistemas

4. Configurar la detección de intrusiones

5. Realizar copias de seguridad de datos y archivos de configuración críticos

6. Crear un equipo que responda a los incidentes relacionados con la seguridad de los equipos

7. Crear un plan de respuesta a incidentes

### Responder a un incidente relacionado con la seguridad

Los pasos básicos que deben seguirse para responder a un incidente relacionado con la seguridad son:

1. Reunir al CSIRT
2. Limitar la propagación de los daños
3. Reunir pruebas detalladas sobre lo ocurrido
4. Reparar los daños y prevenirlos
5. Analizar los sucesos

## 3.24.- Métricas Variables e indicadores.

Las Variables obtenidas para el proceso de ERI se encuentran listadas a continuación.

Tabla 6.- Variables e indicadores del proceso de ERI

| Variables | Descripción. |
|---|---|
| **Xeri1**<br>Frecuencia:<br>Mensualmente | Número de total de sistemas operativos de la organización que necesitan updates<br>Objetivo.- Determinar el número total de sistemas de la organización para poder determinar métricas |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xeri2** Frecuencia:<br>Mensualmente | Número total de sistemas operativos que se les instala sus updates frecuentemente<br>Objetivo.- Ayudará a determinar el porcentaje de sistemas que se actualizan frecuentemente |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xeri3**<br>Frecuencia:<br>6 meses | Costo total de daños que causaron los incidentes de seguridad<br>Objetivo.- Determina el costo total de daños para la empresa por los incidentes de seguridad |
| Fuente: Corporate information security working group | |
| **Xeri4** Frecuencia:<br>Mensualmente | Número de incidentes que se resolvieron siguiendo procesos documentados<br>Objetivo.- Ayudará a determinar una métrica del % de incidentes que se resuelven siguiendo procesos documentados |
| Fuente: Corporate information security working group | |
| **Xeri5**<br>Frecuencia:<br>6 meses | Número de incidentes que ocurren en tiempo determinado<br>Objetivo.- Con base a estadísticas determinar el número de incidentes que ocurren en un tiempo determinado |
| Fuente: Corporate information security working group | |
| **Xeri6**<br>Frecuencia:<br>6 meses | Tiempo en que se revisan los incidentes puede ser 6 meses<br>Objetivo.- Determinar un tiempo de monitoreo de incidentes puede ser cada 6 meses |
| Fuente: Corporate information security working group | |
| **Xeri7**<br>Frecuencia:<br>6 meses | Número de incidentes graves en un período de 6 meses<br>Objetivo.- Determinar el número de incidentes graves que ocurren en un período de tiempo determinado |
| Fuente: Corporate information security working group | |
| **Xeri8**<br>Frecuencia:<br>6 meses | Número de incidentes de gravedad media en un período de 6 meses<br>Objetivo.- Con base a estadísticas determinar el número de incidentes de gravedad media, es decir entre graves y de baja gravedad que ocurren en un tiempo determinado |
| Fuente: Personal | |

| | |
|---|---|
| **Xeri9**<br>Frecuencia:<br>6 meses | Número de incidentes de baja gravedad en un período de 6 meses<br>Objetivo.- Con base a estadísticas determinar el número de incidentes de baja gravedad ocurren en un tiempo determinado |
| Fuente: Personal | |
| **Xeri10**<br>Frecuencia:<br>6 meses | Número de incidentes resueltos en la primera llamada por help-desk en un período de 6 meses<br>Objetivo.- Determinar el porcentaje de incidentes que se resuelven por help-desk en la primera llamada |
| Fuente: Personal | |
| **Xeri11**<br>Frecuencia:<br>6 meses | Tiempo de respuesta en el que se resuelve un incidente desde que se detecta hasta que se soluciona<br>Objetivo.- Determina el tiempo promedio en que se resuelve un incidente desde que se detecta hasta que se soluciona |
| Fuente: Personal | |
| **Xeri12**<br>Frecuencia:<br>6 meses | Número de incidentes de ataques documentados en un período de 6 meses<br>Objetivo.- Determinar el número de ataques que son documentados del total de incidentes ocurridos |
| Fuente: Personal | |
| **Xeri13**<br>Frecuencia:<br>6 meses | Número de incidentes resueltos exitosamente en un período de 6 meses<br>Objetivo.- Determina el número de incidentes que son resueltos exitosamente |
| Fuente: Personal | |
| **Xeri14**<br>Frecuencia:<br>6 meses | Número de incidentes que no son resueltos exitosamente en un período de 6 meses<br>Objetivo.- Determina el número de incidentes que no son resueltos exitosamente |
| Fuente: Personal | |
| **Xeri15**<br>Frecuencia:<br>6 meses | Número de activos que cuentan con bitácora<br>Objetivo.- Determina el número de bitácoras que se pueden monitorear |
| Fuente: Corporate information security working group | |
| **Xeri16**<br>Frecuencia:<br>6 meses | Número de activos que sufren modificaciones en sus bitácoras<br>Objetivo.- Determina el número de activos que sufren modificaciones |
| Fuente: Corporate information security working group | |
| **Xeri17**<br>Frecuencia:<br>6 meses | Número de incidentes de virus, spyware y adware detectados en un período de 6 meses<br>Objetivo.- Determina el número de ataques de virus que ocurren en un tiempo determinado |
| Fuente: Corporate information security working group | |

| | |
|---|---|
| **Xeri18**<br>Frecuencia:<br>6 meses | Número de incidentes de intrusiones por sistema o aplicación en un período de 6 meses<br>Objetivo.- Determina el número de intrusiones que sufre una aplicación o sistema en un tiempo determinado |
| Fuente: Corporate information security working group | |
| **Xeri19**<br>Frecuencia:<br>6 meses | Número de incidentes de ataques a los firewalls en un período de 6 meses<br>Objetivo.- Determina el número de ataques que sufren los firewall en un tiempo determinado |
| Fuente: Corporate information security working group | |
| **Xeri20**<br>Frecuencia:<br>6 meses | Número de incidentes de usos no autorizados en un período de 6 meses<br>Objetivo.- Determina el número de usos no autorizados de aplicaciones o sistemas en un tiempo determinado |
| Fuente: Corporate information security working group | |
| **Xeri21**<br>Frecuencia:<br>6 meses | Número de aplicaciones o programas no autorizados en la empresa en un período de 6 meses<br>Objetivo.- Determina el número de aplicaciones piratas o sin licencia |
| Fuente: Personal | |
| **Xeri22**<br>Frecuencia:<br>6 meses | Número de actualizaciones al programa ERI en un período de 6 meses<br>Objetivo.- Determina si se realizan actualizaciones al programa constantemente |
| Fuente: Personal | |

Algunos indicadores que podemos construir a partir de estas variables son los siguientes.

| Indicadores | Descripción. |
|---|---|
| INDeri1 | Porcentaje total de sistemas operativos que reciben todos sus updates periódicamente<br>Fórmula = Xeri2*100/Xeri1 |
| | |
| INDeri2 | Costo total de daños por incidentes para la organización<br>Fórmula = Xeri3 |
| | |
| INDeri3 | Porcentaje de incidentes que se resuelven siguiendo procesos documentados<br>Fórmula = Xeri4*100/Xeri5 |
| | |
| INDeri4 | Porcentaje de incidentes de impacto grave periódicos<br>Fórmula = (Xeri7*100)/Xeri5 |

| | |
|---|---|
| | |
| | |
| INDeri5 | Porcentaje de incidentes de nivel medio de impacto periódicos<br>Fórmula = (Xeri8*100)/Xeri5 |
| | |
| INDeri6 | Porcentaje de incidentes de bajo impacto periódicos<br>Fórmula = (Xeri9*100)/Xeri5 |
| | |
| INDeri7 | Porcentaje de incidentes que se resuelven por help-desk en la primera llamada en un período de 6 meses<br>Fórmula = Xeri10*100/Xeri5 |
| | |
| INDeri8 | Porcentaje de incidentes documentados periódicamente<br>Fórmula = (Xeri12*100)/Xeri5 |
| | |
| INDeri9 | Porcentaje de incidentes resueltos periódicamente<br>Fórmula = (Xeri13*100)/Xeri1 |
| | |
| INDeri10 | Porcentaje de incidentes no resueltos periódicamente<br>Fórmula = (Xeri14*100)/Xeri1 |
| | |
| INDeri11 | Porcentaje de activos que cuentan con bitácoras<br>Fórmula = (Xeri15*100) / Número total de activos de la organización |
| | |
| INDeri12 | Porcentaje de activos que sufren modificaciones en sus bitácoras Fórmula = (Xeri16*100)/Xeri15 |
| | |
| INDeri13 | porcentaje de incidentes de códigos maliciosos periódicos<br>Fórmula = Xeri17*100/Xeri5 |
| | |
| INDeri14 | Porcentaje de incidentes de intrusiones periódicas<br>Fórmula = Xeri18*100/Xeri5 |

| | |
|---|---|
| | |
| INDeri15 | Porcentaje de incidentes de ataques a firewalls periódicos<br>Fórmula = Xeri19*100/Xeri5 |
| | |
| INDeri16 | Porcentaje de incidentes de usos no autorizados periódicos<br>Fórmula = Xeri20*100/Xeri5 |
| | |
| INDeri17 | Porcentaje de incidentes de aplicaciones o programas no autorizados periódicos<br>Fórmula = Xeri21*100/Xeri5 |
| | |
| INDeri18 | Número de actualizaciones al programa ERI periódicas<br>Fórmula = Xeri18 |
| | |

## *Proceso de control de accesos.*

### 3.25.-Introducción

## 3.25.1.-Seguridad física y lógica.

Es muy importante ser conciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos (hackers, virus, ataques de DoS, etc.); la seguridad de la misma será nula si no se ha previsto como combatir un incendio o cualquier otro tipo de desastre natural y no tener presente políticas claras de recuperación

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos de seguridad física básicos se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de cómputo de la misma, no. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de backup de la sala de cómputo, que intentar acceder vía lógica a la misma.
Así, la Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos

**Las principales amenazas que se prevén en Seguridad Física son:**

1. Desastres naturales, incendios accidentales, tormentas e inundaciones
2. Amenazas ocasionadas por el hombre
3. Disturbios, sabotajes internos y externos deliberados.

   Evaluar y controlar permanentemente la seguridad física de las instalaciones de cómputo y del edificio es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

   **Tener controlado el ambiente y acceso físico permite**:

- Disminuir siniestros
- Trabajar mejor manteniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra accidentes

**Seguridad lógica**

Luego de ver como nuestro sistema puede verse afectado por la falta de seguridad física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra información por él almacenada y procesada.
Así, la seguridad física sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física que la aseguren. Estas técnicas las brinda la Seguridad Lógica.
La Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo".
Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

**Los objetivos que se plantean serán:**

1. Restringir el acceso a los programas y archivos
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Esta información fue obtenida de la pagina de Internet solutions

## 3.26.- Control de accesos.

Como parte de la seguridad lógica, esta el control de accesos. Existen tradicionalmente dos tipos básicos de controles de acceso con filosofías diametralmente opuestas:

* En el modelo de control de acceso discrecional (DAC), un usuario bien identificado (típicamente, el creador o 'propietario' del recurso) decide cómo protegerlo estableciendo cómo compartirlo, mediante controles de acceso impuestos por el sistema. Este es el modelo habitual en buena parte de los sistemas operativos más habituales. Lo esencial es que el propietario del recurso puede cederlo a un tercero.

En sus inicios estos sistemas eran excesivamente simples, al permitir un conjunto limitado de operaciones posibles sobre un recurso (rwx por propietario, grupo o resto de usuarios, como en Unix), si bien pronto se añadieron las famosas listas de control de accesos (ACLs), listas de usuarios y grupos con sus permisos específicos. Las ACLs permiten un nivel de granularidad que, en ocasiones, es inconveniente, por cuanto complica la administración de la seguridad.

* En el modelo de control de acceso mandatorio (MAC), es el sistema quién protege los recursos. Todo recurso del sistema, y todo principal (usuario o entidad del sistema que represente a un usuario) tiene una etiqueta de seguridad. Esta etiqueta de seguridad sigue el modelo de clasificación de la información militar, en donde la confidencialidad de la información es lo más relevante, formando lo que se conoce como política de seguridad multinivel. Una etiqueta de seguridad se compone de una clasificación o nivel de seguridad (número en un rango, o un conjunto de clasificaciones discretas, desde DESCLASIFICADO hasta ALTO SECRETO) y una o más categorías o compartimentos de seguridad (CONTABILIDAD, VENTAS, I+D...). En este tipo de sistemas, todas las decisiones de seguridad las impone el sistema, comparando las etiquetas del accesor frente al recurso accedido, siguiendo un modelo matemático (Bell-LaPadula, 1973). Los criterios de seguridad TCSEC correspondientes al nivel de seguridad B1 o superior incluyen este modelo.

El modelo DAC se ha venido usando profusamente en sistemas operativos de propósito general con clasificación de seguridad TCSEC C1 o superior, y en virtualmente todos los sistemas de bases de datos, aplicativos, y sistemas de comunicaciones de propósito comercial. El modelo MAC no ha salido habitualmente del entorno militar, donde la clasificación de la información es lo más relevante.

Los modelos DAC y MAC son inadecuados para cubrir las necesidades de la mayor parte de las organizaciones. El modelo DAC es demasiado débil para controlar el acceso a los recursos de información de forma efectiva, en tanto que el MAC es demasiado rígido. Desde los 80 se ha propuesto el modelo de control de accesos basado en roles (RBAC), como intento de unificar los modelos clásicos DAC y MAC, consiguiendo un sistema donde el sistema impone el control de accesos, pero sin las restricciones rígidas impuestas por las etiquetas de seguridad.

Básicamente, un rol establece un nivel de in dirección entre los usuarios y los derechos de acceso, a través de un par de relaciones: asignación de roles a usuarios, y asignación de permisos y privilegios a roles. Las políticas de control de accesos basado en roles regulan el acceso de los usuarios a la información en términos de sus actividades y funciones de trabajo, representándose así de forma natural la estructura de las organizaciones.

Uno de los problemas más acuciantes en la gestión de grandes sistemas de información heterogéneos es la complejidad de la administración de seguridad. La aproximación RBAC, intuitivamente, modela de forma natural la estructura de autorización en las organizaciones del mundo real, facilitando las tareas administrativas al separar la asignación de individuos a funciones o perfiles de trabajo, y la definición de políticas de acceso (definición de roles en términos de lo que pueden hacer en el sistema). Permiten asimismo la construcción jerárquica de estas políticas de acceso, por herencia o especialización. Así, la política de control de accesos para un supervisor de planta puede ser una especialización de la del operador de planta. Por ello, la tecnología RBAC tiene el potencial de reducir la complejidad y el coste de la administración de seguridad en estos entornos heterogéneos.

Además, dada la alta integración entre los roles y las responsabilidades de los usuarios, pueden seguirse los principios del mínimo privilegio y de la separación de responsabilidades. Estos principios son vitales para alcanzar el objetivo de integridad, al requerir que a un usuario no se le otorguen mayores privilegios que los necesarios para efectuar su trabajo, y que para completar una transacción de cierta seguridad (por ejemplo, la autorización de un pago) se requiera la culminación de una cadena de transacciones simples por más de un usuario.

El modelo RBAC es hoy día ubicuo: desde sistemas de base de datos relacionales, pasando por sistemas operativos de red, cortafuegos, productos de seguridad mainframe y entornos abiertos, sistemas de Sign-On único y de seguridad web...

La industria ha venido usando otros modelos de control de accesos, como complemento de estos tres básicos, como el modelo de capacidades, en donde parte de las decisiones de autorización se toman a partir de 'capacidades', 'derechos efectivos' o atributos de privilegio, contenidos en las credenciales que un usuario adquiere durante la autenticación. DCE, por ejemplo, incorpora este modelo en su servicio de seguridad. A menudo estos atributos de autorización se integran en un objeto conocido como 'Certificado de Atributos de Privilegio' (PAC, por sus siglas en inglés). Un PAC es como una acreditación de visitante: Se obtiene tras prueba de identidad, está emitida por una autoridad en la que se confía, no identifica al individuo pero sí lo categoriza (e.g. 'Visitante'), es de duración limitada, y no encierra en sí mismo información de privilegios o permisos (qué puertas puedo franquear, por ejemplo) (Rodríguez Luis, 2000).

A continuación se mencionan algunas de las áreas que cubre el control de acceso.

## 3.26.1 Del acceso a áreas críticas.

1. El acceso de personal se llevará acabo de acuerdo a las normas y procedimientos que dicta la Dirección de Telemática.
2. En concordancia con la política de la institución y debido a la naturaleza de estas áreas se llevará un registro permanente del tráfico de personal, sin excepción.
3. La Dirección de Telemática deberá proveer de la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.
4. Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las autoridades superiores de la institución.

## 3.26.2 Del control de acceso al equipo de cómputo.

1. Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.
2. Las áreas donde se tiene equipo de propósito general cuya misión es crítica estarán sujetas a los requerimientos que la Dirección de Telemática emita.
3. Las áreas de cómputo de los departamentos donde se encuentre equipo cuyo propósito reúna características de imprescindible y de misión crítica, deberán sujetarse también a las normas que establezca la Dirección de Telemática.
4. Los accesos a las áreas de críticas deberán de ser clasificados de acuerdo a las normas que dicte la Dirección de Telemática de común acuerdo con su comité de seguridad informática.
5. Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la Dirección de Telemática tiene la facultad de acceder a cualquier equipo de cómputo que no estén bajo su supervisión.

## 3.26.3 Del control de acceso local a la red.

1. El departamento de Cómputo de la Dirección de Telemática es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.
2. La Dirección de Telemática es la responsable de difundir el reglamento para el uso de la red y de procurar su cumplimiento.
3. Dado el carácter unipersonal del acceso a la Empresa, el departamento de Cómputo verificará el uso responsable, de acuerdo al Reglamento para el uso de la red.

4. El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos, equipo de súper computo centralizado y distribuido, etc.) conectado a la red es administrado por el departamento de Cómputo.
5. Todo el equipo de cómputo que esté o sea conectado a la Empresa, o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe de sujetarse a los procedimientos de acceso que emite el departamento de Cómputo.

### 3.26.4 De control de acceso remoto.

1. La Dirección de Telemática es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.
2. Para el caso especial de los recursos de súper cómputo a terceros deberán ser autorizados por la Dirección General o por la Dirección de Vinculación.
3. El usuario de estos servicios deberá sujetarse al Reglamento de uso de la empresa y en concordancia con los lineamientos generales de uso de Internet.
4. El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas que emite la Dirección de Telemática.

### 3.26.5 De acceso a los sistemas administrativos.

1. Tendrá acceso a los sistemas administrativos solo el personal de la empresa que es titular de una cuenta de gastos o bien tenga la autorización del responsable si se trata de personal de apoyo administrativo o técnico.
2. El manejo de información administrativa que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su integridad.
3. Tendrá acceso al sistema de información de la Dirección de Estudios de Postgrado sólo aquellos usuarios de Empresa o externos autorizados por dicha dirección.
4. La instalación y uso de los sistemas de información se rigen por el reglamento de uso de la Empresa y por las normas y procedimientos establecidos por el departamento de Informática.
5. Los servidores de bases de datos administrativos son dedicados, por lo que se prohíben los accesos de cualquiera, excepto para el personal del departamento de Informática.
6. El control de acceso a cada sistema de información de la Dirección Administrativa será determinado por la unidad responsable de generar y procesar los datos involucrados (CICESE, 2001).

## 3.27 Tipos de control de acceso

Algunas medidas de control de acceso específicas se mencionan a continuación.

### El acceso al centro de computación

Si contamos en el edificio con un centro de computación o datacenter deberemos comprobar la seguridad física específica de esa habitación en concreto, por ser esta crítica para nuestros sistemas. Un centro de computación debe tener unas características especiales en cuanto a seguridad que no son necesarias en otros puntos del edificio. Debe tener un sistema de acceso suficientemente seguro, preferiblemente con una puerta blindada y siempre que sea posible con personal de vigilancia que compruebe el acceso por medio de tarjetas de identificación o medios similares. También es posible el uso de sistemas de identificación biométrica, por medio de claves temporales tipo Opie o similares. El acceso físico debe ser todo lo seguro que sea posible, vigilando que la puerta sea lo suficientemente sólida y la cerradura los suficientemente segura. No es difícil el estudio de seguridad física del acceso a un datacenter, pero es complicado el crear un sistema seguro de control de acceso, siendo aconsejable el tener personal de vigilancia que compruebe las identificaciones de forma inequívoca y que apunte en un sistema todos los accesos que se produzcan al datacenter.

### Seguridad física de los backups

De nada sirve mantener un perfecto sistema de backups si cuando es necesario restaurarlos estos no están disponibles. La seguridad física de las cintas o dispositivos de backup debe ser una preocupación para un consultor en seguridad física, y por tanto se debe tener previsto cualquier incidente que se pueda producir, como incendios, terremotos, robos y así cualquier evento que se nos pueda ocurrir.

El sistema más eficaz para mantener los backups seguros es mantenerlos fuera del edificio, o al menos mantener una copia de estos, ya sea en otro edificio o en un centro de almacenamiento de backups. Estos últimos son centros que proporcionan almacenamiento de las cintas de backup con todas las medidas de seguridad física imaginables y que son una buena alternativa al mantenimiento de los backups cerca de las máquinas de las que se ha hecho backup. Puede contratarse uno de estos servicios y mandar los backups o copias de estos a uno de estos servicios, que velará por la seguridad de nuestros backups. Normalmente este tipo de servicios se encarga de ir a la empresa en los períodos de tiempo concertados para recoger las cintas de backup.

Otra alternativa es mantener backups distribuidos, replicando los backups entre edificios o entre sistemas informáticos, para prevenir la perdida de datos por culpa de un problema de seguridad física en alguno de los sistemas o edificios.

**Sistemas de redundancia de servidores y almacenamiento de datos**

Una opción que siempre deberemos considerar cuando realizamos estudios de seguridad física es la posibilidad de mantener varias copias de los datos e incluso tener redundancia para los servidores corporativos. Con los nuevos sistemas de almacenamiento distribuido es sencillo mantener los datos sincronizados en varias localizaciones, con lo que disminuye enormemente la probabilidad de pérdida de datos. Y teniendo suficiente ancho de banda de red para interconectar los sistemas corporativos de varios edificios podemos tener redundancia de los servidores de datos o aplicaciones, con lo que podremos tener la seguridad de que nuestros sistemas informáticos siempre estarán disponibles, aunque no sea en la localización física que estamos estudiando.

La redundancia de servidores y del almacenamiento de los datos, sobre todo cuando está situada en diferentes edificios mejora la seguridad física de un sistema de computación en gran medida, y es una opción a tener en cuenta incluso aunque implementemos otro tipo de sistemas de seguridad física en el edificio.

Los sistemas de gestión y los servidores de aplicaciones comerciales distribuidos son caros y difíciles de mantener hoy en día, pero es posible implementar mediante software libre sistemas distribuidos con precios razonables y con un gran rendimiento. Algunas grandes empresas están liberando bajo licencias de software libre sistemas de gestión de datos distribuidos que pueden ser de gran ayuda en estos casos. Para los sistemas de almacenamiento distribuido existen varias opciones tanto de software libre como de software comercial, por lo que sólo deberemos ocuparnos de tener el sistema adecuado y el ancho de banda suficiente para poder replicar los datos.

El único punto de fallo con estos sistemas es el enlace de comunicación entre los sistemas a replicar, sobre todo cuando manejamos datos críticos. Para solucionar esto debemos aplicar otro tipo de redundancia, tanto en los sistemas como en los enlaces de red entre sistemas, como hemos explicado más arriba

**Acceso físico al hardware**

El acceso físico al hardware sea este computadoras o dispositivos de red deberá ser restringido, teniendo en cuenta las necesidades de cada departamento o usuario. Se debe hacer aquí una distinción entre los equipos de red y servidores departamentales o corporativos y las máquinas de usuario final.

Los equipos de red importantes como enrutadores, pasarelas y concentradores deberán estar en un lugar donde exista un control de acceso, ya sea mediante vigilancia por medio de personas o mediante el aislamiento de las salas o armarios donde estos se encuentren por medio de cerraduras o sistemas de control de acceso mediante tarjetas, claves o control biométrico. Para cada acceso deberá reflejarse una entrada en un sistema de control que puede ser desde un simple libro donde se vayan apuntando las personas y el acceso que han tenido a los equipos hasta un sistema informático que deje reflejado en sus logs el acceso al hardware y quien lo ha hecho. Es importante controlar y reflejar siempre en los apuntes quien ha accedido al hardware, con que motivo y las modificaciones físicas o lógicas que en su caso pueda haber realizado sobre este hardware. Los dispositivos de red que permitan un acceso remoto deberán ser protegidos por medio de claves y cortafuegos para limitar el acceso a las personas que tienen a su cargo la administración de estos sistemas. Se deberá prever la posibilidad de que intrusos o atacantes intenten cambiar la configuración del hardware de red, sobre todo en el caso de enrutadores y concentradores que proporcionen funcionalidad de VPN, para esto se seguirán las medidas de seguridad informática indicadas para cada caso, que dependerán del tipo de dispositivo y de sus posibilidades de configuración. Es esencial el control físico de estos dispositivos porque algunos de ellos permiten el acceso a la configuración por medio de conexión a puertos serie y proporcionan una seguridad menor cuando se accede de esta forma. Se deberá prever también la posibilidad de atacantes con el tiempo suficiente para realizar ataques de fuerza bruta sobre las claves de los sistemas o denegaciones de servicio por medio de envío de tráfico masivo o construido contra los dispositivos. Se debe prever también la posibilidad hoy en día de que estos dispositivos sean hackeados, pues muchos de estos dispositivos tienen su propio sistema operativo o están directamente basados en hardware estándar que es más susceptible a ser atacado por medio de ataques informáticos. Incluso las más modernas impresoras láser cuentan con su propio sistema operativo, que puede ser hackeado y que puede proveer a un atacante de un medio de acceso a la red prácticamente no tenido nunca en cuenta por los administradores encargados de la seguridad.

Para los servidores departamentales o corporativos se deberá tener en cuenta las mismas premisas que para los dispositivos de red y además las propias de cualquier computadora que necesite una seguridad física e informática. Se tendrá en cuenta también la localización física de las máquinas y en su caso se proveerá el mismo control de acceso que para los dispositivos de red importantes.

Una de las medidas más eficaces contra los ataques tanto físicos como informáticos sobre todo este tipo de sistemas es la monitorización continua de los dispositivos mediante sistemas de monitorización basados en hardware o software. Los administradores de la red y de los servidores deberán mantener bajo observación estos dispositivos mediante esta monitorización buscando

fallos y deberá evaluarse en cada caso si el fallo ha sido fortuito o se ha debido a algún tipo de manipulación sobre el hardware o sobre el software de los dispositivos.

Las maquinas de usuario final donde han de trabajar los empleados son paradójicamente las más importantes y las mas difíciles de proteger, porque normalmente han de estar situadas en el entorno del usuario, donde están expuestas a los errores o manipulaciones que un usuario poco cuidadoso o mal informado pueda realizar sobre ellas. En secciones posteriores de este manual se explicará como proteger este tipo de máquinas, pero a nivel corporativo puede ser interesante algún tipo de monitorización también de estas máquinas para detectar fallos o manipulaciones del hardware o el software. La localización de estas máquinas deberá ser idealmente centralizada, en forma de racks o de armarios donde se agrupen las máquinas y donde se pueda controlar el acceso a estas, siempre que los usuarios finales no deban manipular físicamente las máquinas, como en el caso de utilización de lectores de CDROM, grabadoras de CDs o disqueteras. Se intentará siempre que sea posible que el usuario final trabaje de forma remota sobre los servidores de la empresa, implementando soluciones de acceso remoto a las aplicaciones y los datos, o manteniendo como hemos dicho las máquinas en una localización segura donde el usuario no pueda manipularlas.

**Control de acceso al hardware. Control de acceso del personal**

El control de acceso al hardware se realizará preferiblemente mediante personal que verifique mediante algún tipo de identificación a las personas que tienen permiso para acceder al hardware o mediante dispositivos electrónicos (claves, sistemas biométricos) o físicos (puertas blindadas, cerraduras seguras, etc) que permitan controlar quien tiene acceso al hardware y quien no. Es muy útil en estos casos tener una política clara y concisa sobre quien, como, cuando y para que puede tener acceso al hardware. Estas normativas deberán ser conocidas por todo el personal con acceso al hardware y deberán estar plasmadas sobre papel para poder ser consultadas en caso de duda.

Siempre será preferible la intervención de personal encargado del acceso al hardware que la utilización de llaves, tarjetas o dispositivos electrónicos, pues estos últimos son más susceptibles de ser burlados mediante varios sistemas, mientras que los primeros simplemente deberán ser entrenados para evitar el Hackeo Social y para seguir la política de acceso al hardware de manera estricta. En sistemas muy críticos se puede poner personal de vigilancia o cámaras para controlar el acceso al hardware. La rigidez de las políticas de acceso al hardware son inversamente proporcionales a la facilidad de administración de los sistemas, pero normalmente son necesarias si queremos mantener una política de seguridad física alta.

Los dispositivos y servidores situados fuera de los centros de datos o de computación o en las zonas departamentales deberán ser protegidos mediante armarios o racks cerrados con llave y deberá imponerse una política en el departamento de acceso a estos sistemas.

Es importante que en todos los casos siempre tengamos una persona encargada del control del acceso al hardware y que tenga responsabilidades asociadas a este cometido. Puede tratarse de los mismos administradores, de los usuarios (mediante políticas de acceso) o de personal contratado para este cometido. Estas personas deberán responsabilizarse personalmente de todos los accesos al hardware que se produzcan y apuntar en los libros o logs detalladamente todas las manipulaciones realizadas.

Un punto poco conocido pero muy a tener en cuenta en la seguridad física de los sistemas es el control de acceso del personal de mantenimiento del edificio. El personal de limpieza, de mantenimiento del edificio y personal similar debe pasar por los mismos sistemas de control de acceso que los administradores o usuarios de las máquinas. Todo el mundo confía en el personal de limpieza o de mantenimiento, probablemente todo el mundo los conoce y llevan años trabajando en la empresa, pero si nuestros datos son suficientemente críticos haremos bien en desconfiar de todo el mundo, y también de ellos. Alguien puede ofrecer una cantidad de dinero o extorsionar de alguna forma al personal para que extraiga datos o provoque daños en el hardware, todo depende de lo importante que sean nuestros datos y de su valor económico. Incluso pueden producir daños graves por simple desconocimiento, pues no es la primera vez que el personal de limpieza desenchufa un servidor crítico de la empresa para enchufar la aspiradora. Y no es una broma, ocurre de verdad. Lo ideal es que personal de vigilancia acompañe al personal de limpieza y mantenimiento cuando este deba acceder a los centros de computación o a los sitios donde estén alojados servidores o sistemas de almacenamiento de datos. También se puede usar otro tipo de control de acceso como tarjetas o sistemas biométricos, que prevengan este tipo de comportamientos.

**Acceso físico a las máquinas y dispositivos de red**

Es inevitable que el personal tenga acceso físico a las máquinas sobre las que deben trabajar, y en algunos casos incluso a los dispositivos de red. Cuando el usuario debe usar el hardware directamente, como usando disqueteras, CDROOMs o similares la máquina que alberga estos dispositivos debe estar cercana al usuario. Lo mismo es aplicable para los servidores y dispositivos de red y los administradores de sistemas, para poder realizar su trabajo tienen que tener normalmente acceso físico a los dispositivos de red.

Teniendo en cuenta este factor debemos intentar mediante el estudio de la red y de las aplicaciones que han de correr los usuarios finales el mantener al menos los servidores y los dispositivos de red lejos del usuario final, en racks, armarios

o centros de datos. Los usuarios podrán acceder a sus datos a través de la red local y mantener los datos importantes a salvo, aunque el hardware donde van a trabajar este desprotegido por estar en su puesto de trabajo. Los sistemas NAS y otros sistemas de almacenamiento de datos o servidores de aplicaciones pueden ayudar en esto.

Por tanto la idea es mantener al menos los datos y el trabajo del usuario fuera de la máquina donde el usuario va a trabajar. Deberemos instar al personal de administración para que organice el sistema de forma que los usuarios finales trabajen directamente sobre servidores de ficheros y servidores de aplicaciones, manteniendo así los datos a salvo de errores o manipulaciones del hardware. Bien estudiado este sistema puede suponer un ahorro adicional en hardware en las estaciones de trabajo del usuario final, que podrán ser menos complicadas en su constitución y más sencillas de administrar.

**Control remoto de hardware**

El control remoto del hardware podemos verlo desde dos puntos de vista. El punto de vista hardware puro, donde estaríamos hablando de los sistemas SNMP que hemos comentado en el punto anterior o el punto de vista del software, que abarca una gran cantidad de servicios como TELNET, SSH, FTP/SCP/SFTP, Webmin y similares, etc.

En el caso de la seguridad física solo nos interesa la posibilidad de que alguien controle de forma remota nuestro hardware. Esto es cada vez menos común y no debe ser una gran preocupación para el consultor. Uno de los puntos a tener en cuenta es si existen modems conectados a las máquinas que puedan ser accedidos desde el exterior, y por supuesto la conectividad de red desde el exterior, pero estos son puntos más adecuados para el tratamiento por parte del personal de seguridad informática que por el personal de seguridad física.

Nuestra mayor preocupación será por tanto la ocultación dentro de la empresa por un intruso malintencionado de dispositivos como portátiles, pequeños ordenadores tipo Capuccino o similares conectados a nuestra red interna y que puedan servir a un atacante exterior para controlar nuestra red y por tanto nuestro hardware, aunque esta posibilidad es pequeña y casi poco plausible. Los sistemas de seguridad informática deberían detectar este tipo de dispositivos fácilmente y trazarlos hasta ser eliminados.

Se puede hablar también de control remoto del hardware cuando hablamos de virus, troyanos, gusanos o rootkits instalados dentro de la empresa, ya sea a través de la red pública o por usuarios mal formados o malintencionados. Estos sistemas proporcionan a un supuesto atacante exterior control sobre nuestro

software y hardware, pero deberían ser fácilmente detectables por el personal de seguridad informática.

**Acceso a datos técnicos de la red y del hardware**

Aquí tenemos un punto verdaderamente importante dentro de la seguridad física. Hay que ser muy claros en este punto: Nadie que no sea parte del personal de administración de la red y del hardware debe tener acceso a los datos técnicos de la red y del hardware. Si alguien necesita acceso puntual a algún dato se investigará si realmente necesita ese acceso y se concederá el acceso en base a cada petición y con todas las reservas posibles.

Conocer los datos técnicos de la red y del hardware de un sistema proporciona a un supuesto atacante dos facilidades muy apreciadas por estos: La primera es la facilidad que el conocimiento del hardware y la estructura de la red proporciona para realizar ataques informáticos de todo tipo. La segunda es la posibilidad de usar estos datos para usarlos en ataques de Hacking Social, que son tan peligrosos como los ataques informáticos.

Para protegernos de este tipo de ataques debemos mantener la estructura de la red y del hardware (incluido marcas, software instalado, direcciones IP, MACs, etc) secretas o al menos bajo un control de acceso estricto. Uno de los primeros pasos que realiza siempre un hacker antes de atacar un sistema es estudiar la estructura de la red y de las máquinas que la componen. Si ya tiene estos datos tiene la mitad del trabajo hecho, y nosotros la mitad del sistema hackeado... Deberemos por tanto mantener los datos técnicos en armarios a tal efecto, y deberá pedirse permiso al personal de administración de red para acceder a ellos, proporcionando únicamente los datos imprescindibles y apuntando siempre quien ha solicitado los datos y para que. Un buen control de estos datos redundará en una mayor seguridad de todo el sistema. Por parte de los encargados de la seguridad informática deberán considerar cualquier intento de análisis remoto de la estructura de la red o de las máquinas como un intento de intrusión (no hablamos aquí de un simple escaneo de puertos, por supuesto, sino de ataques más sofisticados de recopilación de datos) y por tanto deberán comunicarlo a quien consideren necesario.

Otro peligro son los ataques de hacking social. Un intruso que ha obtenido datos técnicos muy concretos sobre la red de la empresa y sobre el hardware y los ordenadores de la empresa puede hacerse pasar por una persona del servicio técnico de cualquiera de las marcas con las que trabajamos o por personal de otro departamento, proporcionando estos datos a una persona del personal de administración o al usuario final puede convencerlo para que le proporcione otros datos, como claves de acceso o datos que puedan llevarle a conseguir un acceso remoto a nuestros sistemas. El hacking social debe ser considerado como una de las mayores amenazas para la seguridad de los sistemas hoy en día y el mejor arma que tiene un hacker social son los datos, sobre todo si se

trata de datos técnicos que se suponen secretos o únicamente conocidos por el personal de la empresa.

## 3.28.- Métricas variables e indicadores.

Las variables obtenidas para el proceso de control de acceso se listan a continuación.

Tabla 7.- Variables e indicadores del proceso de control de accesos

| Variables | Descripción. |
|---|---|
| **Xca1**<br>Frecuencia:<br>1 año | Número de total de sistemas con que cuenta la organización en un período de 1 año<br>Objetivo.- Determinar el número total de sistemas con que cuenta la organización para poder realizar métricas. |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca2** Frecuencia:<br>1 año | Número de sistemas con controles Técnicos probados en un período de 1 año<br>objetivo .- Determinar el número total de sistemas con controles técnicos probados |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca3**<br>Frecuencia:<br>1 año | Número de sistemas que cuentan con controles TECNICOS desde su implementación<br>Objetivo.- Determinar el número total de sistemas que cuentan con controles técnicos desde su implementación |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca4**<br>Frecuencia:<br>1 año | Número de sistemas que han modificado sus controles TECNICOS desde su implementación<br>Objeto.- Construir una métrica con el número de sistemas que han modificado sus controles técnicos desde su implementación |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca5** Frecuencia:<br>1 año | Número de usuarios con accesos especiales a sistemas en un período de 1 año<br>objetivo.- Determinar el número total de usuarios con accesos especiales para definir métricas |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca6**<br>Frecuencia:<br>1 año | Número total de usuarios con accesos especiales que han sido auditados en un período de 1 año<br>Objetivo.- Determinar si los usuarios con accesos especiales representan una amenaza |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca7** Frecuencia:<br>1 año | Número total de contenedores de medios de respaldo<br>Objetivo.- Determinar el número total de contenedores de medios de respaldo con que cuenta la organización. |

| | |
|---|---|
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca8**<br>Frecuencia:<br>1 año | Número total de contenedores de respaldo que cuentan con logs de deposito y retiro de respaldos<br>Objetivo.- Ayudará determinar un métrica del total de contenedores que cuentan con bitácora |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca9**<br>Frecuencia:<br>1 año | Número total de de instalaciones de telecomunicaciones que cuentan con líneas de transmisión de datos<br>Objetivo.- Determinar el número total de instalaciones de telecomunicaciones con líneas de transmisión de datos |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca10**<br>Frecuencia:<br>1 año | Número total de instalaciones de telecomunicaciones que cuentan con restricciones de acceso para todos sus puntos de entrada<br>Objetivo.- Determinar una métrica del porcentaje total de instalaciones de telecomunicaciones con restricciones de acceso |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca11**<br>Frecuencia:<br>1 año | Número total de PCS en la organización<br>Objetivo.- Determinar el número total de PCS con que cuenta la organización. |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca12**<br>Frecuencia:<br>1 año | Número total de PCS que cuentan con capacidad de encriptación para sus archivos<br>Objetivo.- Construir una métrica que determine el porcentaje de PCS con capacidad de encriptación |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca13**<br>Frecuencia:<br>6 meses | Número total de sistemas con restricciones para el personal de mantenimiento<br>Objetivo.- Determinar una métrica que busque reducir el nivel de riesgo de modificaciones a sistemas por personal de mantenimiento |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca14**<br>Frecuencia:<br>6 meses | Número total de de modificaciones de software en un periodo de 1 año<br>Objetivo.- Determinar el numero total de modificaciones de software |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca15**<br>Frecuencia:<br>6 meses | Número total de modificaciones de software Documentados<br>Objetivo.- Determinar una métrica que determine el porcentaje de cambios en software que son documentados |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |

| | |
|---|---|
| **Xca16**<br>Frecuencia:<br>1 mes | Número de aplicaciones que requieren updates<br>objetivo.- Determinar el numero total de aplicaciones que requieren actualizaciones |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca17**<br>Frecuencia:<br>1 mes | Número de aplicaciones que se les aplicaron todas las actualizaciones en un periodo de un mes<br>Objetivo.- Determinar una métrica de porcentaje del numero de aplicaciones que se les instalaron todas sus actualizaciones |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca18**<br>Frecuencia:<br>1 año | Número total de sistemas que cambiaron el password que traen del fabricante<br>Objetivo.- Determinar una métrica que ayude a minimizar los accesos no autorizados |
| Fuente: Corporate information security working group | |
| **Xca19**<br>Frecuencia:<br>1 año | Número total de sistemas que corren protocolos restringidos.<br>Objetivo.- Ayudara a determinar una métrica para el % de sistemas que corren protocolos restringidos. |
| Fuente: Corporate information security working group | |

Los indicadores que se pueden construir a partir de estas variables se listan a continuación.

| Indicadores | Descripción. |
|---|---|
| INDca1 | Porcentaje total de sistemas que cuentan con controles técnicos probados en un período de 1 año<br>Fórmula = Xca2*100/Xca1 |
| | |
| INDca2 | Porcentaje de sistemas que han modificado sus controles TECNICOS desde su implementación<br>Fórmula = Xca4*100/Xca3 |
| | |
| INDca3 | Porcentaje de usuarios con accesos especiales a sistemas que han sido auditados en un período de 1 año<br>Fórmula = Xca6*100/xca5 |
| | |
| INDca4 | Porcentaje de contenedores de respaldo que cuentan con bitácora<br>Fórmula = Xca8*100/Xca7 |
| | |
| INDca5 | Porcentaje de instalaciones de transmisión en la organización que cuentan con restricción de |

| | |
|---|---|
| | accesos<br>Fórmula = Xca9*100/Xca10 |
| | |
| INDca6 | Porcentaje de PCS con capacidad de encriptación<br>Fórmula = Xca12*100/Xca11 |
| | |
| INDca7 | Porcentaje de sistemas con restricciones al personal de acceso<br>Fórmula = Xca13*100/Xca1 |
| | |
| INDca8 | Porcentaje de cambios de software que son documentados en un período de 1 año<br>Fórmula = Xca15*100/Xca14 |
| | |
| INDca9 | Porcentaje de aplicaciones que recibieron todas sus actualizaciones en un período de 1 mes<br>Fórmula = Xca17*100/Xca16 |
| | |
| INDca10 | Porcentaje de sistemas que cambiaron el password del fabricante Fórmula = Xca18*100/Xca1 |
| | |
| INDca11 | Porcentaje de sistemas que corren protocolos restringidos<br>Fórmula = Xca19*100/Xca1 |
| | |

## *Proceso de administración de riesgos.*

### 3.29.-Introducción

En un entorno informático existen una serie de recursos (humanos, técnicos, de infraestructura.) que están expuestos a diferentes tipos de riesgos: los normales, aquellos comunes a cualquier entorno, y los excepcionales, originados por situaciones concretas que afectan o pueden afectar a parte de una organización o a toda la misma, como la inestabilidad política en un país o una región sensible a terremotos. Para tratar de minimizar los efectos de un problema de seguridad se realiza lo que denominamos un análisis de riesgos, término que hace referencia al proceso necesario para responder a tres cuestiones básicas sobre nuestra seguridad:

- >qué queremos proteger?
- >contra quién o qué lo queremos proteger?
- >cómo lo queremos proteger?

### 3.30.-Enfoques de administración de riesgos

En la práctica existen dos aproximaciones para responder a estas cuestiones, una cuantitativa y otra cualitativa. La primera de ellas es con diferencia la menos usada, ya que en muchos casos implica cálculos complejos o datos difíciles de estimar. Se basa en dos parámetros fundamentales: la probabilidad de que un suceso ocurra y una estimación del coste o las pérdidas en caso de que así sea; el producto de ambos términos es lo que se denomina coste anual estimado (EAC, Estimated Annual Cost), y aunque teóricamente es posible conocer el riesgo de cualquier evento (el EAC) y tomar decisiones en función de estos datos, en la práctica la inexactitud en la estimación o en el cálculo de parámetros hace difícil y poco realista esta aproximación.

El segundo método de análisis de riesgos es el cualitativo, de uso muy difundido en la actualidad especialmente entre las nuevas consultoras de seguridad (aquellas más especializadas en seguridad lógica, cortafuegos, tests de penetración y similares). Es mucho más sencillo e intuitivo que el anterior, ya que ahora no entran en juego probabilidades exactas sino simplemente una estimación de pérdidas potenciales. Para ello se interrelacionan cuatro elementos principales: las amenazas, por definición siempre presentes en cualquier sistema, las vulnerabilidades, que potencian el efecto de las amenazas, el impacto asociado a una amenaza, que indica los daños sobre un activo por la materialización de dicha amenaza, y los controles o salvaguardas, contramedidas para minimizar las vulnerabilidades (controles preventivos) o el impacto (controles curativos). Por ejemplo, una amenaza sería un pirata que queramos o no (no depende de nosotros) va a tratar de modificar nuestra página web principal, el impacto sería una medida del daño que causaría si lo lograra,

una vulnerabilidad sería una configuración incorrecta del servidor que ofrece las páginas, y un control la reconfiguración de dicho servidor o el incremento de su nivel de parcheado. Con estos cuatro elementos podemos obtener un indicador cualitativo del nivel de riesgo asociado a un activo determinado dentro de la organización, visto como la probabilidad de que una amenaza se materialice sobre un activo y produzca un determinado impacto.

En España es interesante la metodología de análisis de riesgo desarrollado desde el Consejo Superior de Informática (Ministerio de Administraciones Públicas) y denominado MAGERIT (Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las administraciones públicas)); se trata de un método formal para realizar un análisis de riesgos y recomendar los controles necesarios para su minimización. MAGERIT se basa en una aproximación cualitativa que intenta cubrir un amplio espectro de usuarios genéricos gracias a un enfoque orientado a la adaptación del mecanismo dentro de diferentes entornos, generalmente con necesidades de seguridad y nivel de sensibilidad también diferentes. En la página web del Consejo Superior de Informática23.2 podemos encontrar información más detallada acerca de esta metodología, así como algunos ejemplos de ejecución de la misma.

**Modelo de análisis de riesgos.**

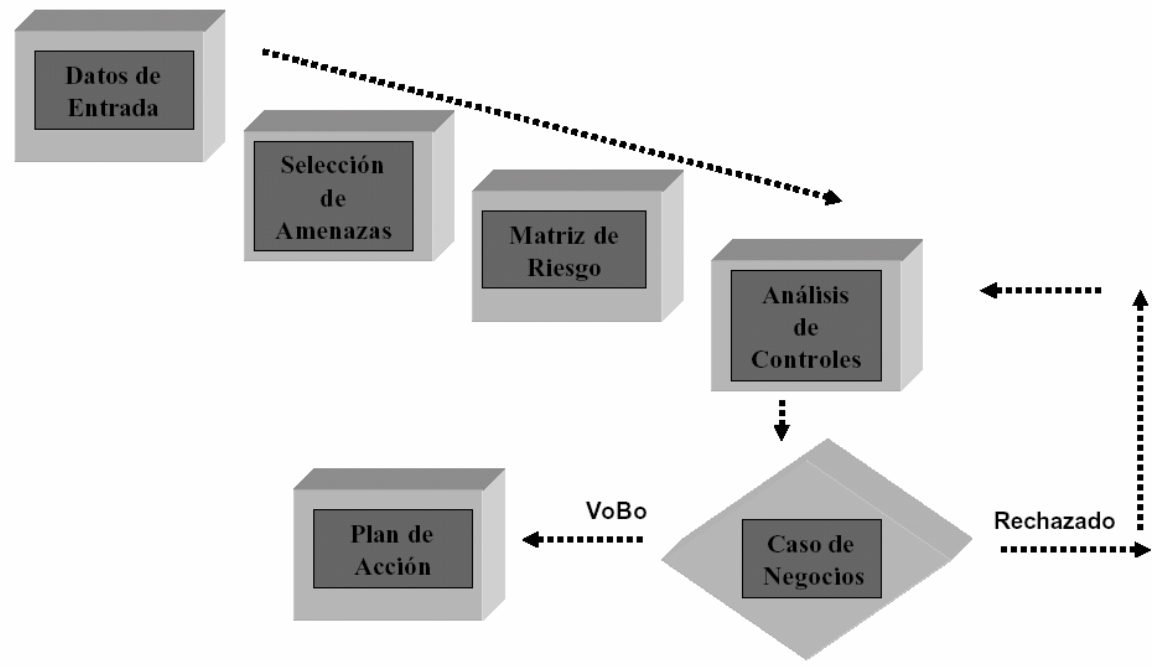



Figura 5.- modelo del análisis de riesgos.

## 3.31.-Evaluación de riesgos

Tras obtener mediante cualquier mecanismo los indicadores de riesgo en nuestra organización llega la hora de evaluarlos para tomar decisiones organizativas acerca de la gestión de nuestra seguridad y sus prioridades. Tenemos por una parte el riesgo calculado, resultante de nuestro análisis, y este riesgo calculado se ha de comparar con un cierto umbral (umbral de riesgo) determinado por la política de seguridad de nuestra organización; el umbral de riesgo puede ser o bien un número o bien una etiqueta de riesgo (por ejemplo, nivel de amenaza alto, impacto alto, vulnerabilidad grave, etc.), y cualquier riesgo calculado superior al umbral ha de implicar una decisión de reducción de riesgo. Si por el contrario el calculado es menor que el umbral, se habla de riesgo residual, y el mismo se considera asumible (no hay porqué tomar medidas para reducirlo). El concepto de asumible es diferente al de riesgo asumido, que denota aquellos riesgos calculados superiores al umbral pero sobre los que por cualquier razón (política, económica...) se decide no tomar medidas de reducción; evidentemente, siempre hemos de huir de esta situación.

Una vez conocidos y evaluados de cualquier forma los riesgos a los que nos enfrentamos podremos definir las políticas e implementar las soluciones prácticas - los mecanismos - para minimizar sus efectos. Vamos a intentar de entrar con más detalle en cómo dar respuesta a cada una de las preguntas que nos hemos planteado al principio de este punto:

### Identificación de recursos

Debemos identificar todos los recursos cuya integridad pueda ser amenazada de cualquier forma; por ejemplo:

- Hardware
  Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, ordenadores personales, impresoras, unidades de disco, líneas de comunicación, servidores, enrutadores
- Software
  Códigos fuente y objeto, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicación...
- Información
  En ejecución, almacenada en línea, almacenada fuera de línea, en comunicación, bases de datos...
- Personas
  Usuarios, operadores.
- Accesorios
  Papel, cintas, tóners.

Aparte del recurso en sí (algo tangible, como un enrutadores) hemos de considerar la visión intangible de cada uno de estos recursos (por ejemplo la

capacidad para seguir trabajando sin ese enrutadores). Es difícil generar estos aspectos intangibles de los recursos, ya que es algo que va a depender de cada organización, su funcionamiento, sus seguros, sus normas...No obstante, siempre hemos de tener en cuenta algunos aspectos comunes: privacidad de los usuarios, imagen pública de la organización, reputación, satisfacción del personal y de los clientes - en el caso de una universidad, de los alumnos -, capacidad de procesamiento ante un fallo. Con los recursos correctamente identificados se ha de generar una lista final, que ya incluirá todo lo que necesitamos proteger en nuestra organización.

**Identificación de amenazas**

Una vez conocemos los recursos que debemos proteger es la hora de identificar las vulnerabilidades y amenazas que se ciernen contra ellos. Una vulnerabilidad es cualquier situación que pueda desembocar en un problema de seguridad, y una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad; entre ambas existe una estrecha relación: sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.

Se suelen dividir las amenazas que existen sobre los sistemas informáticos en tres grandes grupos, en función del ámbito o la forma en que se pueden producir:

- Desastres del entorno.

  Dentro de este grupo se incluyen todos los posibles problemas relacionados con la ubicación del entorno de trabajo informático o de la propia organización, así como con las personas que de una u otra forma están relacionadas con el mismo. Por ejemplo, se han de tener en cuenta desastres naturales (terremotos, inundaciones.), desastres producidos por elementos cercanos, como los cortes de fluido eléctrico, y peligros relacionados con operadores, programadores o usuarios del sistema.

- Amenazas en el sistema.

  Bajo esta denominación se contemplan todas las vulnerabilidades de los equipos y su software que pueden acarrear amenazas a la seguridad, como fallos en el sistema operativo, medidas de protección que éste ofrece, fallos en los programas, copias de seguridad...

- Amenazas en la red.

Cada día es menos común que una máquina trabaje aislada de todas las demás; se tiende a comunicar equipos mediante redes locales, intranets o la propia Internet, y esta interconexión acarrea nuevas - y peligrosas - amenazas a la seguridad de los equipos, peligros que hasta el momento de la conexión no se suelen tener en cuenta. Por ejemplo, es necesario analizar aspectos relativos al cifrado de los datos en tránsito por la red, a proteger una red local del resto de internet, o a instalar sistemas de autenticación de usuarios remotos que necesitan acceder a ciertos recursos internos a la organización (como un investigador que conecta desde su casa a través de un módem).

Algo importante a la hora de analizar las amenazas a las que se enfrentan nuestros sistemas es analizar los potenciales tipos de atacantes que pueden intentar violar nuestra seguridad. Es algo normal que a la hora de hablar de atacantes todo el mundo piense en crackers, en piratas informáticos mal llamados hackers. No obstante, esto no es más que el fruto de la repercusión que en todos los medios tienen estos individuos y sus acciones; en realidad, la inmensa mayoría de problemas de seguridad vienen dados por atacantes internos a la organización afectada. En organismos de I+D estos atacantes suelen ser los propios estudiantes (rara vez el personal), así como piratas externos a la entidad que aprovechan la habitualmente mala protección de los sistemas universitarios para acceder a ellos y conseguir así cierto status social dentro de un grupo de piratas. Los conocimientos de estas personas en materias de sistemas operativos, redes o seguridad informática suelen ser muy limitados, y sus actividades no suelen entrañar muchos riesgos a no ser que se utilicen nuestros equipos para atacar a otras organizaciones, en cuyo caso a los posibles problemas legales hay que sumar la mala imagen que nuestras organizaciones adquieren.

No siempre hemos de contemplar a las amenazas como actos intencionados contra nuestro sistema: muchos de los problemas pueden ser ocasionados por accidentes, desde un operador que derrama una taza de café sobre una terminal hasta un usuario que tropieza con el cable de alimentación de un servidor y lo desconecta de la línea eléctrica, pasando por temas como el borrado accidental de datos o los errores de programación; decir `no lo hice a propósito' no ayuda nada en estos casos. Por supuesto, tampoco tenemos que reducirnos a los accesos no autorizados al sistema: un usuario de nuestras máquinas puede intentar conseguir privilegios que no le corresponden, una persona externa a la organización puede lanzar un ataque de negación de servicio contra la misma sin necesidad de conocer ni siquiera un login y una contraseña, etc.

**Medidas de protección**

Tras identificar todos los recursos que deseamos proteger, así como las posibles vulnerabilidades y amenazas a que nos exponemos y los potenciales atacantes que pueden intentar violar nuestra seguridad, hemos de estudiar cómo proteger nuestros sistemas, sin ofrecer aún implementaciones concretas para protegerlos (esto ya no serían políticas sino mecanismos). Esto implica en primer lugar cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades de que una amenaza se pueda convertir en realidad. Este cálculo puede realizarse partiendo de hechos sucedidos con anterioridad en nuestra organización, aunque por desgracia en muchos lugares no se suelen registrar los incidentes acaecidos. En este caso, y también a la hora de evaluar los daños sobre recursos intangibles, existen diversas aproximaciones como el método Delphi, que básicamente consiste en preguntar a una serie de especialistas de la organización sobre el daño y las pérdidas que cierto problema puede causar; no obstante, la experiencia del administrador en materias de seguridad suele tener aquí la última palabra a la hora de evaluar los impactos de cada amenaza.

La clasificación de riesgos de cara a estudiar medidas de protección suele realizarse en base al nivel de importancia del daño causado y a la probabilidad aproximada de que ese daño se convierta en realidad; se trata principalmente de no gastar más dinero en una implementación para proteger un recurso de lo que vale dicho recurso o de lo que nos costaría recuperarnos de un daño en él o de su pérdida total. Por ejemplo, podemos seguir un análisis similar en algunos aspectos al problema de la mochila: llamamos al riesgo de perder un recurso i (a la probabilidad de que se produzca un ataque), y le asignamos un valor de 0 a 10 (valores más altos implican más probabilidad); de la misma forma, definimos también de 0 a 10 la importancia de cada recurso, siendo 10 la importancia más alta. La evaluación del riesgo es entonces el producto de ambos valores, llamado peso o riesgo evaluado de un recurso, y medido en dinero perdido por unidad de tiempo (generalmente, por año):

De esta forma podemos utilizar hojas de trabajo en las que, para cada recurso, se muestre su nombre y el número asignado, así como los tres valores anteriores. Evidentemente, los recursos que presenten un riesgo evaluado mayor serán los que más medidas de protección deben poseer, ya que esto significa que es probable que sean atacados, y que además el ataque puede causar pérdidas importantes. Es especialmente importante un grupo de riesgos denominados inaceptables, aquellos cuyo peso supera un cierto umbral; se trata de problemas que no nos podemos permitir en nuestros sistemas, por lo que su prevención es crucial para que todo funcione correctamente.

Una vez que conocemos el riesgo evaluado de cada recurso es necesario efectuar lo que se llama el análisis de costes y beneficios. Básicamente consiste en comparar el coste asociado a cada problema (calculado anteriormente, ) con el coste de prevenir dicho problema. El cálculo de este último no suele ser complejo si conocemos las posibles medidas de prevención que tenemos a nuestra disposición: por ejemplo, para saber lo que nos cuesta prevenir los efectos de un incendio en la sala de operaciones, no tenemos más que consultar los precios de sistemas de extinción de fuego, o para saber lo que nos cuesta proteger nuestra red sólo hemos de ver los precios de productos como enrutadores que bloqueen paquetes o cortafuegos completos. No sólo hemos de tener en cuenta el coste de cierta protección, sino también lo que nos puede suponer su implementación y su mantenimiento; en muchos casos existen soluciones gratuitas para prevenir ciertas amenazas, pero estas soluciones tienen un coste asociado relativo a la dificultad de hacerlas funcionar correctamente de una forma continua en el tiempo, por ejemplo dedicando a un empleado a su implementación y mantenimiento.

## 3.32.-Apoyo a la toma de decisiones

Cuando ya hemos realizado este análisis no tenemos más que presentar nuestras cuentas a los responsables de la organización (o adecuarlas al presupuesto que un departamento destina a materias de seguridad), siempre teniendo en cuenta que el gasto de proteger un recurso ante una amenaza ha de ser inferior al gasto que se produciría si la amenaza se convirtiera en realidad. Hemos de tener siempre presente que los riesgos se pueden minimizar, pero nunca eliminarlos completamente, por lo que será recomendable planificar no sólo la prevención ante de un problema sino también la recuperación si el mismo se produce; se suele hablar de medidas proactivas (aquellas que se toman para prevenir un problema) y medidas reactivas (aquellas que se toman cuando el daño se produce, para minimizar sus efectos).

## 3.33.-Implementación de controles

Sólo hay una información de la fase de apoyo a la toma de decisiones necesaria para la fase de implementación de controles: la lista de prioridades de soluciones de control que se tienen que implementar. Si ha seguido los procedimientos descritos en el capítulo 5, "Apoyo a la toma de decisiones", el equipo de administración de riesgos de seguridad ha registrado esta información y ha presentado sus resultados al comité directivo de seguridad.

### Participantes en la fase de implementación de controles

Los participantes de esta fase son, principalmente, los responsables de mitigación; sin embargo, pueden obtener ayuda del equipo de administración de riesgos de seguridad. La fase de implementación de controles incluye las siguientes funciones, que se han definido en el capítulo 3, "Información general acerca de la administración de riesgos de seguridad":

- Equipo de administración de riesgos de seguridad (grupo de seguridad de información, responsable de evaluación de riesgos y responsable de registro de evaluación de riesgos)
- Responsables de mitigación (arquitectura de TI, ingeniería de TI y operaciones de TI)

En la siguiente lista se resumen las responsabilidades específicas:

- **Ingeniería de TI**: determina el modo en que se implementan las soluciones de control
- **Arquitectura de TI**: especifica el modo en que las soluciones de control se implementarán de una manera compatible con los sistemas informáticos existentes
- **Operaciones de TI**: implementa soluciones de control técnico
- **Seguridad de la información**: contribuye a resolver los problemas que se puedan producir durante las pruebas y la implementación
- **Finanzas**: garantiza que los niveles de gasto estén dentro de los presupuestos aprobados

Como práctica recomendada, el equipo de administración de riesgos de seguridad debe asignar un técnico de seguridad para cada riesgo identificado. Un único punto de contacto reduce el riesgo de que el equipo de administración de riesgos de seguridad genere mensajes incoherentes y ofrezca un modelo de compromiso nítido a lo largo del proceso de implementación.

### Herramientas proporcionadas para la fase de implementación de controles

No hay herramientas incluidas en esta guía relacionadas con la fase de implementación de controles.

### Resultados necesarios para la fase de implementación de controles

Durante esta fase del proceso de administración de riesgos de seguridad creará planes para implementar las soluciones de control especificadas durante la fase de apoyo a la toma de decisiones. En la tabla siguiente se resumen estos elementos clave y en las secciones posteriores de este capítulo también se resumen.

### Resultados necesarios para la fase de implementación de controles

| Información que se recopilará | Descripción |
|---|---|
| Soluciones de control | Lista de controles seleccionados por el comité directivo de seguridad e implementados por los responsables de mitigación |
| Informes de la implementación de los controles | Informe o serie de informes creados por los responsables de mitigación donde se describe su progreso en la implementación de las soluciones de control seleccionadas |

### Organización de las soluciones de control

El capítulo anterior se ha centrado en el proceso de apoyo a la toma de decisiones. El resultado del análisis en dicha fase han sido las decisiones que el comité directivo de seguridad ha adoptado en relación con el modo en que la organización responderá a los riesgos de seguridad identificados durante la anterior fase de evaluación de riesgos. Puede que algunos riesgos se hayan aceptado o se hayan derivado a terceros; en el caso de los riesgos que se tengan que contrarrestar, se ha creado una lista de prioridades de las soluciones de control.

El siguiente paso consiste en diseñar planes de acción para implementar los controles en un período de tiempo explícito. Estos planes deben ser claros y precisos; además, cada uno se debe asignar a la persona o equipo adecuados para su ejecución. Utilice prácticas de administración de proyectos efectivas para realizar un seguimiento del progreso y garantizar una consecución puntual de los objetivos del proyecto.

## 3.33.-Medición y efectividad del programa

Una vez implementados los controles, resulta importante asegurarse de que proporcionan la protección prevista y de que continúan aplicándose. Por ejemplo, sería una sorpresa desagradable descubrir que la causa principal de una infracción de seguridad importante ha sido que el mecanismo de autenticación de la red privada virtual (VPN) ha permitido que los usuarios no autenticados tuvieran acceso a la red corporativa porque no se ha configurado correctamente durante la implementación. Incluso sería un descubrimiento todavía más desagradable saber que los intrusos han obtenido acceso a los recursos internos porque un ingeniero de la red ha vuelto a configurar un servidor de seguridad para permitir protocolos adicionales sin obtener aprobación previa mediante el proceso de control de cambios de la organización.

## 3.34.-Métricas variables e indicadores.

Las variables obtenidas para el proceso de Análisis de riesgos se listan a continuación.

Tabla 8.- Variables e indicadores del proceso de IRM

| Variables | Descripción. |
|---|---|
| **Xirm1**<br>Frecuencia:<br>1 año | Número total de sistemas con los que cuenta la empresa<br>Objetivo.- Determinar el número total de sistemas con los que cuenta la empresa |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xirm2** Frecuencia:<br>1 año | Número de sistemas que se les aplica un IRM en un período de 1 año<br>Objetivo.- Conocer el número total de sistemas que se les aplica un IRM |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xirm3**<br>Frecuencia:<br>1 año | Número de sistemas que cuentan con IRM documentado en un período de 1 año<br>Objetivo.- Conocer el número total de sistemas que tienen IRM documentado |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xirm4** Frecuencia:<br>1 año | Número de riesgos del total de sistemas, que son aceptados y no se les da seguimiento<br>Objetivo: Determinar el número total de riesgos del total de sistemas que no se les da seguimiento por alguna razón |
| Fuente: Personal | |
| **Xirm5**<br>Frecuencia:<br>1 año | Número de riesgos mitigados en un período de 1 año<br>Objetivo.- Determinar el número de riesgos mitigados en un período de 1 año |
| Fuente: Personal | |
| **Xirm6** Frecuencia:<br>1 año | Número de vulnerabilidades o debilidades descubiertas en un período de 1 año<br>Objetivo.- Utilizar esta variable para determinar tiempo promedio de respuesta entre que la debilidad es descubierto y la implementación de la acción correctiva<br>datos necesarios # vulnerabilidades que se detectan en 30, 60,90, 180,360 días |
| Fuente: Personal | |
| **Xirm7**<br>Frecuencia:<br>1 año | Número de sistemas con IRM que son revisados por dirección general en un período de 1 año<br>Objetivo.- Determinar el grado de involucramiento de la dirección |
| Fuente: Personal | |
| **Xirm8** Frecuencia:<br>1 año | Número de activos críticos para los cuales el costo por daño perdida ha sido cuantificado en un período de 1 año<br>Objetivo.- Determinar el número de activos totales cuyo costo por daño o perdida ha sido cuantificado |
| Fuente: Personal | |

| | |
|---|---|
| **Xirm9**<br>Frecuencia:<br>1 año | Número de riesgos que están relacionados con amenazas externas en un período de un 1 año<br>Objetivo.- ayudará a determinar el porcentaje de amenazas externas |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xirm10**<br>Frecuencia:<br>1 año | Número de nuevas vulnerabilidades que se les da seguimiento desde el último reporte<br>Objetivo.- Determinar el número total de vulnerabilidades que se les da seguimiento desde el último reporte |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |

Los indicadores que se pueden construir a partir de estas variables son los siguientes.

| Indicadores | Descripción. |
|---|---|
| INDirm1 | Porcentaje de sistemas que se les aplico un IRM en un período de 1 año<br>Fórmula = (Xirm2*100)/Xirm1 |
| | |
| INDirm2 | Porcentaje de sistemas que cuentan con IRM documentado en un período de 1 año<br>Fórmula = (Xirm3*100/Xirm1 |
| | |
| INDirm3 | Porcentaje de riesgos en sistemas que no se les da seguimiento en un período de 1 año<br>Fórmula = Xirm4*100/Xirm1 |
| | |
| INDirm4 | Porcentaje de riesgos mitigados en un período de 1 año<br>Fórmula = Xirm5*100/total de riesgos detectados en un año |
| | |
| INDirm5 | Tiempo promedio entre que una vulnerabilidad es descubierta y la implementación de acción correctiva<br>Fórmula=(Xirm6*30+Xirm6*60+Xirm6*90+Xirm6*180+Xirm6*360)/Suma de Xirm6(30,60,90,180,360) |
| | |
| INDirm6 | Porcentaje de sistemas con IRM revisados por dirección en un período de 1 año<br>Fórmula = Xirm7*100/Xirm2 |
| | |
| INDirm7 | Porcentaje de activos cuyo costo por daño o perdida ha sido cuantificado<br>Fórmula = Xirm8*100 / Número total de activos |
| | |
| INDirm8 | Porcentaje de riesgos externos en un período de 1 año |

| | |
|---|---|
| | Fórmula = Xirm9*100/ Número de riesgos detectados en un período de 1 año |
| | |
| INDirm9 | Porcentaje de nuevas vulnerabilidades que se les da seguimiento desde el último reporte<br>Fórmula = Xirm10*100 / Número total de vulnerabilidades descubiertas desde el último reporte |
| | |

# Capitulo 4.- Variables

## *Definición de variables e indicadores.*

### 4.1.-resultados

A continuación se muestra un resumen todas las variables encontradas en cada uno de los procesos, las métricas o indicadores que se pueden construir se encuentran al final de cada lista de variables.

Tabla 9.- Resumen de variables e indicadores

### 4.2.-Proceso concientización.

Las variables son

| Variables | Descripción. |
|---|---|
| **Xcon1**<br>Frecuencia:<br>6 Meses | Número de empleados Totales de la organización.<br>Objetivo.- Considera el número total de empleados de la organización para realizar estadísticas en base a ese número. |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xcon2**<br>Frecuencia:<br>6 Meses | Período de tiempo en que se realizan las revisiones o auditorias al proceso de concientización en promedio será 6 meses.<br>Objetivo.- Establece un período de tiempo específico para realizar las revisiones o auditorias del proceso de concientización en promedio será 6 meses. |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xcon3**<br>Frecuencia:<br>6 Meses | Número de empleados que reciben capacitación sobre concientización en un período de 6 meses.<br>Objetivo.- Determinar el porcentaje de la población total de empleados que reciben capacitación en concientización. |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xcon4**<br>Frecuencia:<br>6 Meses | Número de Actividades de concientización que se realizan en un período de 6 meses.<br>Objetivo.- Determina si el número de actividades que pueden ser campañas, programas, cursos, conferencias que se realizan en un período de tiempo son suficientes |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xcon5**<br>Frecuencia:<br>6 Meses | Número de audiencias creadas para las diferentes actividades de concientización en un período de 6 meses<br>Objetivo.- Determina si se han creado suficientes números de audiencias para cubrir las necesidades especificas en determinados tipos de empleados |
| Fuente: Personal | |
| **Xcon6** | Número de empleados que asisten por audiencia en un período de 6 meses. |

| | |
|---|---|
| Frecuencia:<br>6 Meses | Objetivo.- Determinar el porcentaje total de empleados de determinada área que asisten por audiencia. |
| Fuente: Personal | |
| **Xcon7**<br>Frecuencia:<br>6 Meses | Número total de tópicos que buscan revisarse en las actividades de concientización.<br>Objetivo.- Determinar el número total de tópicos que quieren revisarse en los cursos de capacitación. |
| Fuente: Personal | |
| **Xcon8**<br>Frecuencia:<br>6 Meses | Número de tópicos que realmente se ven en las actividades de concientización.<br>Objetivo: Determinar el número de tópicos que se ven en las actividades de concientización. |
| Fuente: Personal | |
| **Xcon9**<br>Frecuencia:<br>6 Meses | Número de actividades de concientización a las que asiste un empleado en un período de 6 meses.<br>Objetivo.- Determinar el número de actividades totales a las que asistió un empleado |
| Fuente: Personal | |
| **Xcon10**<br>Frecuencia:<br>6 Meses | Total de horas que dura un empleado en entrenamiento en un período de 6 meses<br>Objetivo: Tener el número total de horas de entrenamiento que recibe un empleado |
| Fuente: Personal | |
| **Xcon11**<br>Frecuencia:<br>6 Meses | Número total de empleados que asisten a mas horas de entrenamiento en actividades de concientización<br>Objetivo.- Determinar el número de horas promedios a las que asisten los empleados a actividades de concientización |
| Fuente: Personal | |
| **Xcon12**<br>Frecuencia:<br>6 Meses | Número de empleados que presentan las encuestas y exámenes de concientización en un período de 6 meses<br>Objetivo: Determina el número de empleados total que presentan las encuestas y exámenes |
| Fuente: Corporate information security working group | |
| **Xcon13**<br>Frecuencia:<br>6 Meses | Número de empleados que contestan correctamente las encuestas de concientización en un período de 6 meses<br>Objetivo.- Determinar que la cantidad de empleados que contestan correctamente las encuestas y exámenes |
| Fuente: Corporate information security working group | |

| | |
|---|---|
| **Xcon14**<br>Frecuencia:<br>6 Meses | Número de reportes de incidentes levantados en un período de 6 meses<br>Objetivo: Determina en que porcentaje hay un incremento o disminución de reportes de incidentes de seguridad debido al proceso de concientización |
| Fuente: Personal | |
| **Xcon15**<br>Frecuencia:<br>6 Meses | Número de personas que han tomado cursos de concientización y que levantaron reporte de incidentes en un período de 6 meses<br>Objetivo.- Expresa el número de personas concientizadas que levantan reportes de inseguridad |
| Fuente: Personal | |

Los indicadores son

| Indicadores | Descripción. |
|---|---|
| INDCon1 | Porcentaje de personal sometido a cursos de concientización.<br>Fórmula = (Xcon3*100)/Xcon1 |
| | |
| INDCon2 | Actividades de concientizacion periódicas (cada 6 meses)<br>Fórmula = Xcon4 |
| | |
| INDCon3 | Audiencias creadas por período de tiempo (5 meses)<br>Fórmula = Xcon5 |
| | |
| INDCon4 | Porcentaje de personas en determinada área que asiste por audiencia periódicamente (6 meses)<br>Fórmula = (Xcon6*100)/número total de empleados de determinada área. |
| | |
| INDCon5 | Porcentaje de cubrimiento de los tópicos en actividades de concientizacion<br>Fórmula = Con8*100/Xcon7 |
| | |
| INDCon6 | Número de horas promedio que dura un empleado en actividades de concientización<br>Fórmula = Xcon10*Xcon9 (Esta métrica es por empleado) |
| | |
| INDCon7 | Número total de empleados que asisten a mas horas de entrenamiento en actividades de concientización<br>Fórmula = Xcon11 |
| | |

| | |
|---|---|
| INDCon8 | Porcentaje de personas que aprueban las encuestas<br>Fórmula = (Xcon13*100)/Xcon12 |
| | |
| INDCon9 | Porcentaje de incremento o disminución de reportes de incidentes que se levantaron periódicamente (cada 6 meses)<br>Fórmula = Xcon14 – (Número del último reporte de incidentes) |
| | |
| INDCon10 | Número de personas que han tomado cursos de concientización y que levantan reportes de incidentes<br>Fórmula = Xcon15 |
| | |

## 4.3.-Proceso de plan de continuidad del negocio.

Las variables son

| Variables | Descripción. |
|---|---|
| **Xbcp1**<br>Frecuencia:<br>1 año | Número de total de aplicaciones críticas que requieren respaldo<br>Objetivo.- Determinar el número total de aplicaciones que requieren respaldo |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xbcp2**<br>Frecuencia:<br>1 año | Número total de aplicaciones críticas que son respaldados frecuentemente de acuerdo a la norma<br>Objetivo.- Ayudará a determinar el porcentaje de aplicaciones críticas que requieren respaldo |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xbcp3**<br>Frecuencia:<br>1 año | Número de total de sistemas de la organización<br>Objetivo.- Determinar el número total de sistemas de la organización |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xbcp4**<br>Frecuencia:<br>1 año | Número total de sistemas que cuentan con un plan de contingencia.<br>Objetivo.- Ayudará a determinar el % total de sistemas con un plan de contingencia |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xbcp5**<br>Frecuencia:<br>1 año | Número de total de sistemas de gestión de negocio que tienen planes de contingencia probados<br>Objetivo.- Ayudará a construir una métrica del % de planes de contingencias probados. |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xbcp6**<br>Frecuencia: | Número total de unidades organizacionales<br>Objetivo.- Determinar el número total de unidades organizacionales para obtener métricas |

| | |
|---|---|
| 1 año | |
| Fuente: Corporate information security working group | |
| **Xbcp7**<br>Frecuencia:<br>1 año | Número de total de unidades organizacionales que cuentan con un plan de continuidad<br>Objetivo.- Ayudará a obtener un a métrica del porcentaje de unidades organizacionales que cuentan con un plan |
| Fuente: Corporate information security working group | |
| **Xbcp8**<br>Frecuencia:<br>1 año | Número total de unidades organizacionales que cuentan con un plan de continuidad documentado.<br>Objetivo.- Ayudará a determinar una métrica del porcentaje de unidades organizacionales que cuentan con un BCP documentado |
| Fuente: Corporate information security working group | |
| **Xbcp9**<br>Frecuencia:<br>1 año | Número de total de planes de BCP de unidades de negocios que son auditados<br>Objetivo.- Ayudará a obtener un a métrica del % de BCP de unidades organizacionales que son auditados |
| Fuente: Corporate information security working group | |
| **Xbcp10**<br>Frecuencia:<br>1 año | Número total de planes de BCP de unidades de negocios que son actualizados<br>Objetivo.- Determinar una métrica del % de BCP de unidades organizacionales que son Actualizados |
| Fuente: Corporate information security working group | |

Los indicadores son

| Indicadores | Descripción. |
|---|---|
| INDbcp1 | Porcentaje de aplicaciones críticas que son respaldados frecuentemente.<br>Fórmula = Xbcp2*100/Xbcp1 |
| | |
| INDbcp2 | Porcentaje de sistemas que cuentan con un plan de contingencia Fórmula = Xbcp4*100/Xbcp3 |
| | |
| INDbcp3 | Porcentaje de planes de contingencias probados<br>Fórmula = Xbcp5*100/Xbcp3 |

| | |
|---|---|
| | |
| INDbcp4 | Porcentaje de unidades organizacionales que cuentan con un Plan de continuidad<br>Fórmula = Xbcp7*100/Xbcp6 |
| | |
| INDbcp5 | Porcentaje de unidades organizacionales con un BCP documentado.<br>Fórmula = Xbcp8*100/Xbcp6 |
| | |
| INDbcp6 | Porcentaje de BCP de unidades de negocios que son auditados<br>Fórmula = Xbcp9*100/Xbcp7 |
| | |
| INDbcp7 | Porcentaje de BCP de unidades de negocios que son actualizados.<br>Fórmula = Xbcp10*100/Xbcp7 |
| | |

## 4.4.-Proceso de política de seguridad de información.

Las variables son

| Variables | Descripción. |
|---|---|
| **Xpol1**<br>Frecuencia:<br>6 meses | Número de total de sistemas con passwords<br>Objetivo.- Determinar el número total de sistemas con passwords de la organización para elaborar métricas |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xpol2** Frecuencia:<br>6 meses | Número total de sistemas que cuentan con política de password<br>Objetivo.- Ayudará a determinar el % de sistemas que cuentan con política de password |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xpol3**<br>Frecuencia:<br>6 meses | Número de total de websites con los que cuenta la organización<br>Objetivo.- Determinar el número total de websites con los que cuenta la organización para poder obtener métricas |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xpol4** Frecuencia:<br>6 meses | Número total de websites que cuentan con política de seguridad incorporada<br>Objetivo.- Ayudará a determinar el % de websites que cuentan con política de seguridad incorporada |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xpol5**<br>Frecuencia:<br>6 meses | Número de proveedores o de outsourcing con los que tiene relación la empresa<br>Objetivo.- Determinar el número total de proveedores o de outsourcing para poder establecer métricas |

| | |
|---|---|
| Fuente: Corporate information security working group | |
| **Xpol6**<br>Frecuencia:<br>6 meses | Número de proveedores o de outsourcing con los que se ha establecido una políticas de seguridad para el intercambio de información<br>Objetivo.- Determinar el % de proveedores o outsourcing con los que se han establecido políticas de seguridad. |
| Fuente: Corporate information security working group | |
| **Xpol7** Frecuencia:<br>6 meses | Número de políticas corporativas totales que existen en la organización<br>Objetivo.- Determinar el número total de políticas corporativas que existen en una organización |
| Fuente: Corporate information security working group | |
| **Xpol8**<br>Frecuencia:<br>6 meses | Número de políticas especificas que han sido violadas por los usuarios<br>Objetivo.- Ayudará a determinar el % de políticas que han sido violadas |
| Fuente: Corporate information security working group | |
| **Xpol9** Frecuencia:<br>6 meses | Número de políticas que son actualizadas<br>Objetivo.- Determinar una métrica del % de políticas Actualizadas |
| Fuente: Personal | |
| **Xpol10**<br>Frecuencia:<br>1 año | Número de políticas que son auditadas<br>Objetivo.- Determinar una métrica del % de políticas auditadas |
| Fuente: Personal | |
| **Xpol11**<br>Frecuencia:<br>1 año | Número de políticas nuevas creadas<br>Objetivo.- Determinar el número de nuevas políticas creadas en un período de tiempo determinado |
| Fuente: Corporate information security working group | |
| **Xpol12**<br>Frecuencia:<br>1 año | Número de aplicaciones que cuentan con procedimiento de respaldo en la organización<br>Objetivo.- Determina el número total de aplicaciones con procedimiento de respaldo con que cuenta la empresa |
| Fuente: Corporate information security working group | |
| **Xpol13**<br>Frecuencia:<br>1 año | Número de aplicaciones cuyo respaldos se realizan de acuerdo a la política de respaldo<br>Objetivo.- Determinar una métrica del % de aplicaciones con procedimientos de respaldos que se apegan a la política. |
| Fuente: Corporate information security working group | |

Los indicadores son

| Indicadores | Descripción. |
|---|---|
| INDpol1 | Porcentaje de sistemas con política de password<br>Fórmula = Xpol2*100/Xpol1 |
| | |
| INDpol2 | Porcentaje de websites que cuentan con política de seguridad<br>Frecuencia = Xpol4*100/Xpol3 |
| | |
| INDpol3 | Porcentaje de proveedores o de outsourcing con los que se han desarrollado políticas de seguridad<br>Fórmula = Xpol6*100/Xpol5 |
| | |
| INDpol4 | Porcentaje de políticas especificas que han sido violadas por los usuarios<br>Fórmula = Xpol8*100/Xpol7 |
| | |
| INDpol5 | Porcentaje de políticas actualizadas<br>Fórmula = Xpol9*100/Xpol7 |
| | |
| INDpol6 | Porcentaje de políticas que son auditadas<br>Fórmula = Xpol10*100/Xpol7 |
| | |
| INDpol7 | Número de políticas nuevas creadas periódicamente<br>Fórmula = Xpol11 |
| | |
| INDpol8 | Porcentaje de aplicaciones con procedimiento de respaldo que se apega a la política de respaldo<br>Fórmula = Xpol13*100/Xpol11 |
| | |

## 4.5.-Proceso de respuesta de incidentes

Las variables son

| Variables | Descripción. |
|---|---|
| **Xeri1**<br>Frecuencia:<br>Mensualmente | Número de total de sistemas operativos de la organización que necesitan updates<br>Objetivo.- Determinar el número total de sistemas de la organización para poder determinar métricas |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xeri2** Frecuencia:<br>Mensualmente | Número total de sistemas operativos que se les instala sus updates frecuentemente<br>Objetivo.- Ayudará a determinar el porcentaje de sistemas que se actualizan frecuentemente |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xeri3**<br>Frecuencia:<br>6 meses | Costo total de daños que causaron los incidentes de seguridad<br>Objetivo.- Determina el costo total de daños para la empresa por los incidentes de seguridad |
| Fuente: Corporate information security working group | |
| **Xeri4** Frecuencia:<br>Mensualmente | Número de incidentes que se resolvieron siguiendo procesos documentados<br>Objetivo.- Ayudará a determinar una métrica del % de incidentes que se resuelven siguiendo procesos documentados |
| Fuente: Corporate information security working group | |
| **Xeri5**<br>Frecuencia:<br>6 meses | Número de incidentes que ocurren en tiempo determinado<br>Objetivo.- Con base a estadísticas determinar el número de incidentes que ocurren en un tiempo determinado |
| Fuente: Corporate information security working group | |
| **Xeri6**<br>Frecuencia:<br>6 meses | Tiempo en que se revisan los incidentes puede ser 6 meses<br>Objetivo.- Determinar un tiempo de monitoreo de incidentes puede ser cada 6 meses |
| Fuente: Corporate information security working group | |
| **Xeri7**<br>Frecuencia:<br>6 meses | Número de incidentes graves en un período de 6 meses<br>Objetivo.- Determinar el número de incidentes graves que ocurren en un período de tiempo determinado |
| Fuente: Corporate information security working group | |
| **Xeri8**<br>Frecuencia:<br>6 meses | Número de incidentes de gravedad media en un período de 6 meses<br>Objetivo.- Con base a estadísticas determinar el número de incidentes de gravedad media, es decir entre graves y de baja gravedad que ocurren en un tiempo determinado |
| Fuente: Personal | |
| **Xeri9**<br>Frecuencia:<br>6 meses | Número de incidentes de baja gravedad en un período de 6 meses<br>Objetivo.- Con base a estadísticas determinar el número de incidentes de baja gravedad ocurren en un tiempo determinado |

| | |
|---|---|
| Fuente: Personal | |
| **Xeri10**<br>Frecuencia:<br>6 meses | Número de incidentes resueltos en la primera llamada por help-desk en un período de 6 meses<br>Objetivo.- Determinar el porcentaje de incidentes que se resuelven por help-desk en la primera llamada |
| Fuente: Personal | |
| **Xeri11**<br>Frecuencia:<br>6 meses | Tiempo de respuesta en el que se resuelve un incidente desde que se detecta hasta que se soluciona<br>Objetivo.- Determina el tiempo promedio en que se resuelve un incidente desde que se detecta hasta que se soluciona |
| Fuente: Personal | |
| **Xeri12**<br>Frecuencia:<br>6 meses | Número de incidentes de ataques documentados en un período de 6 meses<br>Objetivo.- Determinar el número de ataques que son documentados del total de incidentes ocurridos |
| Fuente: Personal | |
| **Xeri13**<br>Frecuencia:<br>6 meses | Número de incidentes resueltos exitosamente en un período de 6 meses<br>Objetivo.- Determina el número de incidentes que son resueltos exitosamente |
| Fuente: Personal | |
| **Xeri14**<br>Frecuencia:<br>6 meses | Número de incidentes que no son resueltos exitosamente en un período de 6 meses<br>Objetivo.- Determina el número de incidentes que no son resueltos exitosamente |
| Fuente: Personal | |
| **Xeri15**<br>Frecuencia:<br>6 meses | Número de activos que cuentan con bitácora<br>Objetivo.- Determina el número de bitácoras que se pueden monitorear |
| Fuente: Corporate information security working group | |
| **Xeri16**<br>Frecuencia:<br>6 meses | Número de activos que sufren modificaciones en sus bitácoras<br>Objetivo.- Determina el número de activos que sufren modificaciones |
| Fuente: Corporate information security working group | |
| **Xeri17**<br>Frecuencia:<br>6 meses | Número de incidentes de virus, spyware y adware detectados en un período de 6 meses<br>Objetivo.- Determina el número de ataques de virus que ocurren en un tiempo determinado |
| Fuente: Corporate information security working group | |

| | |
|---|---|
| **Xeri18**<br>Frecuencia:<br>6 meses | Número de incidentes de intrusiones por sistema o aplicación en un período de 6 meses<br>Objetivo.- Determina el número de intrusiones que sufre una aplicación o sistema en un tiempo determinado |
| Fuente: Corporate information security working group | |
| **Xeri19**<br>Frecuencia:<br>6 meses | Número de incidentes de ataques a los firewalls en un período de 6 meses<br>Objetivo.- Determina el número de ataques que sufren los firewall en un tiempo determinado |
| Fuente: Corporate information security working group | |
| **Xeri20**<br>Frecuencia:<br>6 meses | Número de incidentes de usos no autorizados en un período de 6 meses<br>Objetivo.- Determina el número de usos no autorizados de aplicaciones o sistemas en un tiempo determinado |
| Fuente: Corporate information security working group | |
| **Xeri21**<br>Frecuencia:<br>6 meses | Número de aplicaciones o programas no autorizados en la empresa en un período de 6 meses<br>Objetivo.- Determina el número de aplicaciones piratas o sin licencia |
| Fuente: Personal | |
| **Xeri22**<br>Frecuencia:<br>6 meses | Número de actualizaciones al programa ERI en un período de 6 meses<br>Objetivo.- Determina si se realizan actualizaciones al programa constantemente |
| Fuente: Personal | |

Los indicadores son

| Indicadores | Descripción. |
|---|---|
| INDeri1 | Porcentaje total de sistemas operativos que reciben todos sus updates periódicamente<br>Fórmula = Xeri2*100/Xeri1 |
| | |
| INDeri2 | Costo total de daños por incidentes para la organización<br>Fórmula = Xeri3 |
| | |
| INDeri3 | Porcentaje de incidentes que se resuelven siguiendo procesos documentados<br>Fórmula = Xeri4*100/Xeri5 |
| | |
| INDeri4 | Porcentaje de incidentes de impacto grave periódicos<br>Fórmula = (Xeri7*100)/Xeri5 |
| | |

| | |
|---|---|
| INDeri5 | Porcentaje de incidentes de nivel medio de impacto periódicos<br>Fórmula = (Xeri8*100)/Xeri5 |
| | |
| INDeri6 | Porcentaje de incidentes de bajo impacto periódicos<br>Fórmula = (Xeri9*100)/Xeri5 |
| | |
| INDeri7 | Porcentaje de incidentes que se resuelven por help-desk en la primera llamada en un período de 6 meses<br>Fórmula = Xeri10*100/Xeri5 |
| | |
| INDeri8 | Porcentaje de incidentes documentados periódicamente<br>Fórmula = (Xeri12*100)/Xeri5 |
| | |
| INDeri9 | Porcentaje de incidentes resueltos periódicamente<br>Fórmula = (Xeri13*100)/Xeri1 |
| | |
| INDeri10 | Porcentaje de incidentes no resueltos periódicamente<br>Fórmula = (Xeri14*100)/Xeri1 |
| | |
| INDeri11 | Porcentaje de activos que cuentan con bitácoras<br>Fórmula = (Xeri15*100) / Número total de activos de la organización |
| | |
| INDeri12 | Porcentaje de activos que sufren modificaciones en sus bitácoras Fórmula = (Xeri16*100)/Xeri15 |
| | |
| INDeri13 | porcentaje de incidentes de códigos maliciosos periódicos<br>Fórmula = Xeri17*100/Xeri5 |
| | |
| INDeri14 | Porcentaje de incidentes de intrusiones periódicas<br>Fórmula = Xeri18*100/Xeri5 |

| | |
|---|---|
| | |
| INDeri15 | Porcentaje de incidentes de ataques a firewalls periódicos<br>Fórmula = Xeri19*100/Xeri5 |
| | |
| INDeri16 | Porcentaje de incidentes de usos no autorizados periódicos<br>Fórmula = Xeri20*100/Xeri5 |
| | |
| INDeri17 | Porcentaje de incidentes de aplicaciones o programas no autorizados periódicos<br>Fórmula = Xeri21*100/Xeri5 |
| | |
| INDeri18 | Número de actualizaciones al programa ERI periódicas<br>Fórmula = Xeri18 |
| | |

## 4.6.-Proceso de control de acceso.

Las variables son

| Variables | Descripción. |
|---|---|
| **Xca1**<br>Frecuencia:<br>1 año | Número de total de sistemas con que cuenta la organización en un período de 1 año<br>Objetivo.- Determinar el número total de sistemas con que cuenta la organización para poder realizar métricas. |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca2** Frecuencia:<br>1 año | Número de sistemas con controles Técnicos probados en un período de 1 año<br>objetivo .- Determinar el número total de sistemas con controles técnicos probados |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca3**<br>Frecuencia:<br>1 año | Número de sistemas que cuentan con controles TECNICOS desde su implementación<br>Objetivo.- Determinar el número total de sistemas que cuentan con controles técnicos desde su implementación |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca4**<br>Frecuencia:<br>1 año | Número de sistemas que han modificado sus controles TECNICOS desde su implementación<br>Objeto.- Construir una métrica con el número de sistemas que han modificado sus controles técnicos desde su implementación |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca5** Frecuencia:<br>1 año | Número de usuarios con accesos especiales a sistemas en un período de 1 año<br>objetivo.- Determinar el número total de usuarios con accesos especiales para definir métricas |

| | |
|---|---|
| | |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca6**<br>Frecuencia:<br>1 año | Número total de usuarios con accesos especiales que han sido auditados en un período de 1 año<br>Objetivo.- Determinar si los usuarios con accesos especiales representan una amenaza |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca7** Frecuencia:<br>1 año | Número total de contenedores de medios de respaldo<br>Objetivo.- Determinar el número total de contenedores de medios de respaldo con que cuenta la organización. |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca8**<br>Frecuencia:<br>1 año | Número total de contenedores de respaldo que cuentan con logs de deposito y retiro de respaldos<br>Objetivo.- Ayudará determinar un métrica del total de contenedores que cuentan con bitácora |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca9**<br>Frecuencia:<br>1 año | Número total de de instalaciones de telecomunicaciones que cuentan con líneas de transmisión de datos<br>Objetivo.- Determinar el número total de instalaciones de telecomunicaciones con líneas de transmisión de datos |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca10**<br>Frecuencia:<br>1 año | Número total de instalaciones de telecomunicaciones que cuentan con restricciones de acceso para todos sus puntos de entrada<br>Objetivo.- Determinar una métrica del porcentaje total de instalaciones de telecomunicaciones con restricciones de acceso |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca11**<br>Frecuencia:<br>1 año | Número total de PCS en la organización<br>Objetivo.- Determinar el número total de PCS con que cuenta la organización. |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca12**<br>Frecuencia:<br>1 año | Número total de PCS que cuentan con capacidad de encriptación para sus archivos<br>Objetivo.- Construir una métrica que determine el porcentaje de PCS con capacidad de encriptación |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca13**<br>Frecuencia:<br>6 meses | Número total de sistemas con restricciones para el personal de mantenimiento<br>Objetivo.- Determinar una métrica que busque reducir el nivel de riesgo de modificaciones a sistemas por personal de mantenimiento |

| | |
|---|---|
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca14**<br>Frecuencia:<br>6 meses | Número total de de modificaciones de software en un periodo de 1 año<br>Objetivo.- Determinar el numero total de modificaciones de software |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca15**<br>Frecuencia:<br>6 meses | Número total de modificaciones de software Documentados<br>Objetivo.- Determinar una métrica que determine el porcentaje de cambios en software que son documentados |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca16**<br>Frecuencia:<br>1 mes | Número de aplicaciones que requieren updates<br>objetivo.- Determinar el numero total de aplicaciones que requieren actualizaciones |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca17**<br>Frecuencia:<br>1 mes | Número de aplicaciones que se les aplicaron todas las actualizaciones en un periodo de un mes<br>Objetivo.- Determinar una métrica de porcentaje del numero de aplicaciones que se les instalaron todas sus actualizaciones |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xca18**<br>Frecuencia:<br>1 año | Número total de sistemas que cambiaron el password que traen del fabricante<br>Objetivo.- Determinar una métrica que ayude a minimizar los accesos no autorizados |
| Fuente: Corporate information security working group | |
| **Xca19**<br>Frecuencia:<br>1 año | Número total de sistemas que corren protocolos restringidos.<br>Objetivo.- Ayudara a determinar una métrica para el % de sistemas que corren protocolos restringidos. |
| Fuente: Corporate information security working group | |

Los indicadores son

| Indicadores | Descripción. |
|---|---|
| INDca1 | Porcentaje total de sistemas que cuentan con controles técnicos probados en un período de 1 año<br>Fórmula = Xca2*100/Xca1 |
| | |
| INDca2 | Porcentaje de sistemas que han modificado sus controles TECNICOS desde su implementación<br>Fórmula = Xca4*100/Xca3 |
| | |
| INDca3 | Porcentaje de usuarios con accesos especiales a sistemas que han sido auditados en un período de 1 año |

| | |
|---|---|
| | Fórmula = Xca6*100/xca5 |
| | |
| INDca4 | Porcentaje de contenedores de respaldo que cuentan con bitácora<br>Fórmula = Xca8*100/Xca7 |
| | |
| INDca5 | Porcentaje de instalaciones de transmisión en la organización que cuentan con restricción de accesos<br>Fórmula = Xca9*100/Xca10 |
| | |
| INDca6 | Porcentaje de PCS con capacidad de encriptación<br>Fórmula = Xca12*100/Xca11 |
| | |
| INDca7 | Porcentaje de sistemas con restricciones al personal de acceso<br>Fórmula = Xca13*100/Xca1 |
| | |
| INDca8 | Porcentaje de cambios de software que son documentados en un período de 1 año<br>Fórmula = Xca15*100/Xca14 |
| | |
| INDca9 | Porcentaje de aplicaciones que recibieron todas sus actualizaciones en un período de 1 mes<br>Fórmula = Xca17*100/Xca16 |
| | |
| INDca10 | Porcentaje de sistemas que cambiaron el password del fabricante Fórmula = Xca18*100/Xca1 |
| | |
| INDca11 | Porcentaje de sistemas que corren protocolos restringidos<br>Fórmula = Xca19*100/Xca1 |
| | |

## 4.7.-Proceso de análisis de riesgos.

Las variables son

| Variables | Descripción. |
|---|---|
| **Xirm1**<br>Frecuencia:<br>1 año | Número total de sistemas con los que cuenta la empresa<br>Objetivo.- Determinar el número total de sistemas con los que cuenta la empresa |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xirm2** Frecuencia:<br>1 año | Número de sistemas que se les aplica un IRM en un período de 1 año<br>Objetivo.- Conocer el número total de sistemas que se les aplica un IRM |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xirm3**<br>Frecuencia:<br>1 año | Número de sistemas que cuentan con IRM documentado en un período de 1 año<br>Objetivo.- Conocer el número total de sistemas que tienen IRM documentado |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xirm4** Frecuencia:<br>1 año | Número de riesgos del total de sistemas, que son aceptados y no se les da seguimiento<br>Objetivo: Determinar el número total de riesgos del total de sistemas que no se les da seguimiento por alguna razón |
| Fuente: Personal | |
| **Xirm5**<br>Frecuencia:<br>1 año | Número de riesgos mitigados en un período de 1 año<br>Objetivo.- Determinar el número de riesgos mitigados en un período de 1 año |
| Fuente: Personal | |
| **Xirm6** Frecuencia:<br>1 año | Número de vulnerabilidades o debilidades descubiertas en un período de 1 año<br>Objetivo.- Utilizar esta variable para determinar tiempo promedio de respuesta entre que la debilidad es descubierto y la implementación de la acción correctiva<br>datos necesarios # vulnerabilidades que se detectan en 30, 60,90, 180,360 días |
| Fuente: Personal | |
| **Xirm7**<br>Frecuencia:<br>1 año | Número de sistemas con IRM que son revisados por dirección general en un período de 1 año<br>Objetivo.- Determinar el grado de involucramiento de la dirección |
| Fuente: Personal | |
| **Xirm8** Frecuencia:<br>1 año | Número de activos críticos para los cuales el costo por daño perdida ha sido cuantificado en un período de 1 año<br>Objetivo.- Determinar el número de activos totales cuyo costo por daño o perdida ha sido cuantificado |

| | |
|---|---|
| Fuente: Personal | |
| **Xirm9**<br>Frecuencia:<br>1 año | Número de riesgos que están relacionados con amenazas externas en un período de un 1 año<br>Objetivo.- ayudará a determinar el porcentaje de amenazas externas |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |
| **Xirm10**<br>Frecuencia:<br>1 año | Número de nuevas vulnerabilidades que se les da seguimiento desde el último reporte<br>Objetivo.- Determinar el número total de vulnerabilidades que se les da seguimiento desde el último reporte |
| Fuente: NIST (Security self- Assessment guide for information technology systems | |

Los indicadores son

| Indicadores | Descripción. |
|---|---|
| INDirm1 | Porcentaje de sistemas que se les aplico un IRM en un período de 1 año<br>Fórmula = (Xirm2*100)/Xirm1 |
| | |
| INDirm2 | Porcentaje de sistemas que cuentan con IRM documentado en un período de 1 año<br>Fórmula = (Xirm3*100/Xirm1 |
| | |
| INDirm3 | Porcentaje de riesgos en sistemas que no se les da seguimiento en un período de 1 año<br>Fórmula = Xirm4*100/Xirm1 |
| | |
| INDirm4 | Porcentaje de riesgos mitigados en un período de 1 año<br>Fórmula = Xirm5*100/total de riesgos detectados en un año |
| | |
| INDirm5 | Tiempo promedio entre que una vulnerabilidad es descubierta y la implementación de acción correctiva<br>Fórmula=(Xirm6*30+Xirm6*60+Xirm6*90+Xirm6*180+Xirm6*360)/Suma de Xirm6(30,60,90,180,360) |
| | |
| INDirm6 | Porcentaje de sistemas con IRM revisados por dirección en un período de 1 año<br>Fórmula = Xirm7*100/Xirm2 |
| | |
| INDirm7 | Porcentaje de activos cuyo costo por daño o perdida ha sido cuantificado<br>Fórmula = Xirm8*100 / Número total de activos |
| | |

| | |
|---|---|
| INDirm8 | Porcentaje de riesgos externos en un período de 1 año<br>Fórmula = Xirm9*100/ Número de riesgos detectados en un período de 1 año |
| | |
| INDirm9 | Porcentaje de nuevas vulnerabilidades que se les da seguimiento desde el último reporte<br>Fórmula = Xirm10*100 / Número total de vulnerabilidades descubiertas desde el último reporte |
| | |

# Capitulo 5.- Caso practico

## *Caso practico Empresa de Telecomunicaciones.*

### 5.1.-Introducción

Después de varias revisiones al conjunto de variables se dejaron las mas significativas, primeramente debemos aclarar que las variables que se han mencionado hasta el momento cumplen una función general, es decir, las variables citadas pueden ser utilizadas en general por cualquier empresa para su monitoreo, pero la manera de medirlas puede variar un poco debido a que cada empresa tiene una forma distintiva de llevar a cabo sus procesos, en algunos casos la estructura de estos procesos pudiera tener algunas variantes ya que cada empresa tiene sus propias metodologías de implementación y tiene su propia forma de documentación, estas variables pueden ser modificadas para ser adaptadas a la manera en que los procesos dentro de determinada empresa se lleva a cabo. Sin embargo, es muy importante que los procesos estén desarrollados bajo metodologías convenientes.

Algunas metodologías pueden ser las siguientes:

| Proceso | Metodología |
|---|---|
| Concientización | Diseños de sistemas de instrucción (ISD). |
| BCM | Metodología de Business Continuity Institute |
| Políticas | Ejemplo de política del CICESE |
| CSIRT | Metodología del CSIRT |
| Control de Accesos | Ejemplos de SANS Institute |
| Análisis de riesgos | Metodología de NIST<br>Metodología de SANS<br>Metodología de Microsoft |

Para poder determinar la valides de estas variables, se presento este conjunto de variables a un grupo de expertos en seguridad de información de una reconocida empresa de telecomunicaciones para que pudieran determinar la factibilidad de estas variables.

Cabe mencionar que algunas de estas variables fueron aceptadas, algunas otras modificadas, y otras mas no fueron utilizadas, pero al analizar las variables que no se tomaron en cuenta se pudieron definir algunas otras que si eran de interés para la empresa.

## 5.2.- Metodología utilizada.

- Definir los procesos con los que cuenta la empresa.
- Determinar si estos procesos están desarrollados bajo metodologías adecuadas.
- Revisar la estructura de los procesos e ir identificando si las variables pueden ser monitoreadas.
- Determinar las variables finales
- Construcción de métricas (Indicadores)
- Revisión final de variables e indicadores.

En este caso la empresa cumple con todos los procesos mencionados en este trabajo, y con todos los demás puntos que se mencionan , los resultados finales se muestran a continuación.

Las variables que fueron de interés para la empresa quedaron definidas de la siguiente forma.

Tabla 10.- Resumen de variables e indicadores del caso practico

## 5.3.- Resultado proceso de concientizacion

Las variables son

| Variables | Descripción. |
|---|---|
| **X´con1**<br>Frecuencia:<br>6 Meses | Número de empleados Totales de la organización.<br>Objetivo.- Considera el número total de empleados de la organización para realizar estadísticas en base a ese número |
| Con relación a Xcon1 | |
| **X´con2**<br>Frecuencia:<br>6 Meses | Período de tiempo en que se realizan las revisiones o auditorias al proceso de concientizacion en promedio será 6 meses<br>Objetivo.- Establece un período de tiempo específico para realizar las revisiones o auditorias del proceso de concientizacion en promedio será 6 meses mínimo, pero puede ser más tiempo. |
| Con relación a Xcon2 | |
| **X´con3**<br>Frecuencia:<br>6 Meses | Número de empleados que reciben capacitación sobre concientizacion en un período de 6 meses<br>Objetivo.- Determinar el porcentaje de la población total de empleados que reciben capacitación en concientizacion |
| Con relación a Xcon3 | |
| **X´con4**<br>Frecuencia:<br>6 Meses | Número de empleados que recibe una constancia de acreditación al final de una sesión de entrenamiento.<br>Objetivo.- Determina el número de personas que obtienen una acreditación interna, esto puede ser aprobar un examen al final de sesión de entrenamiento. |

| | |
|---|---|
| Con relación a Xcon12 | |
| **X´con5**<br>Frecuencia:<br>6 Meses | Número de audiencias creadas para las diferentes actividades de concientizacion en un período de 6 meses<br>Objetivo.- Determina si se han creado suficientes números de audiencias para cubrir las necesidades especificas en determinados tipos de empleados |
| Con relación a Xcon5 | |
| **X´con6**<br>Frecuencia:<br>6 Meses | Número total de personas por audiencia que ya recibió capacitación customizada para el grupo de audiencia al cual pertenece.<br>Objetivo.- Determina el número de personas por audiencia que ya han sido capacitadas considerando el total de personas que se encuentran en esa audiencia. |
| Con relación a Xcon6 | |
| **X´con7**<br>Frecuencia:<br>6 Meses | Número total de tópicos que buscan revisarse en las actividades de concientizacion.<br>Objetivo: Determinar el número total de tópicos que quieren revisarse en los cursos de capacitación |
| Con relación a Xcon7 | |
| **X´con8**<br>Frecuencia:<br>6 Meses | Número de tópicos que realmente se ven en las actividades de concientizacion<br>Objetivo: Determinar el número de tópicos que se ven en las actividades de concientizacion |
| Con relación a Xcon8 | |
| **X´con9**<br>Frecuencia:<br>6 Meses | número de actividades de concientizacion a las que asiste un empleado en un período de 6 meses<br>objetivo.- Determinar el número de actividades totales a las que asistió un empleado |
| Con relación a Xcon9 | |
| **X´con10**<br>Frecuencia:<br>6 Meses | Número total de empleados que asisten a más horas de entrenamiento en actividades de concientizacion.<br>Objetivo.- Determinar número de horas promedios a las que asisten los empleados a actividades de concientizacion. |
| Con relación a Xcon10 | |
| **X´con11**<br>Frecuencia:<br>6 Meses | Número de reportes de incidentes levantados en un período de 6 meses<br>Objetivo.- Determinar en que porcentaje hay un incremento o disminución de reportes de incidentes de seguridad debido al proceso de concientizacion |
| Con relación a Xcon14 | |

Algunos indicadores podemos construir a partir de estas variable son los siguientes.

| Indicadores | Descripción. |
|---|---|
| IND´Con1 | Porcentaje de personal sometido a cursos de concientización<br>Fórmula = (X´con3*100)/X´con1 |

| | |
|---|---|
| | |
| IND´Con2 | Porcentaje de personas que recibe una acreditación<br>Fórmula = (X´con4*100)/X´con3 |
| | |
| IND´Con3 | Audiencias creadas por período de tiempo (6 meses)<br>Fórmula = X´con5 |
| | |
| IND´Con4 | Porcentaje de personas en determinada área que asiste por audiencia periódicamente (6 meses)<br>Fórmula = (X´con6*100)/número total de empleados de determinada área. |
| | |
| IND´Con5 | Porcentaje de cubrimiento de los tópicos en actividades de concientizacion<br>Fórmula =X´Con8*100/X´con7 |
| | |
| IND´Con6 | Número de horas promedio que dura un empleado en actividades de concientizacion<br>Fomula = X´con10*X´con9 (Esta métrica es por empleado) |
| | |
| IND´Con7 | Porcentaje de incremento o disminución de reportes de incidentes que se levantaron periódicamente (cada 6 meses)<br>Fórmula = X´con11 – (Número del último reporte de incidentes) |
| | |

## 5.4.- Resultados del proceso de plan de continuidad.

Las variables son

| | |
|---|---|
| **X´bcp1**<br>Frecuencia:<br>1 año | Número de total de procesos de negocio dentro de la organización.<br>Objetivo. Determinar el número total de procesos de negocio que cuentan con un plan de recuperación |
| Con relación a Xbcp1 | |
| **X´bcp2**<br>Frecuencia:<br>1 año | Número total de procesos de negocio que cuentan con un plan de recuperación detallado.<br>Objetivo.- Determinar el porcentaje de procesos de negocio que cuentan con un plan detallado de recuperación, |
| Con relación a Xbcp2 | |
| **X´bcp3**<br>Frecuencia:<br>1 año | Número total de sistemas de la organización<br>Objetivo. - Determinar el número total de sistemas de la organización. |
| Con relación a Xbcp3 | |

| | |
|---|---|
| **X´bcp4**<br>Frecuencia:<br>1 año | Número total de sistemas que cuentan con un plan de contingencia.<br>Objetivo.- Ayudará a determinar el % total de sistemas con un plan de contingencia |
| Con relación a Xbcp4 | |
| **X´bcp5**<br>Frecuencia:<br>1 año | Número total de sistemas gestión de negocio que tienen planes de contingencia probados<br>Objetivo.- Ayudará a construir una métrica del % de planes de contingencias probados. |
| Con relación a Xbcp5 | |
| **X´bcp6**<br>Frecuencia:<br>1 año | Número total procesos de negocios dentro de la organización.<br>Objetivo.- Determinar el número total de procesos de negocio de dentro de la organización. |
| Con relación a Xbcp6 | |
| **X´bcp7**<br>Frecuencia:<br>1 año | Número total de procesos de negocio que cuentan con un plan de continuidad<br>Objetivo.- Ayudará a obtener un a métrica del porcentaje de procesos de negocio que cuentan con un plan de continuidad. |
| Con relación a Xbcp7 | |
| **X´bcp8**<br>Frecuencia:<br>1 año | Número total de procesos de negocio que cuentan con un plan de continuidad documentado.<br>Objetivo.- Ayudará a determinar una métrica del porcentaje de procesos de negocio que cuentan con un BCP documentado |
| Con relación a Xbcp8 | |
| **X´bcp9**<br>Frecuencia:<br>1 año | Número total de planes de BCP de procesos de negocio que son auditados<br>Objetivo.- Ayudará a determinar una métrica del % de BCP de procesos de negocio que son auditados |
| Con relación a Xbcp9 | |
| **X´bcp10**<br>Frecuencia:<br>1 año | Número total de planes de BCP de procesos de negocio que son actualizados<br>Objetivo.- Determinar una métrica del % de BCP de procesos de negocio que son Actualizados |
| Con relación a Xbcp10 | |

Las métricas que se pueden construir a partir de estas variables son las siguientes.

| Indicadores | Descripción. |
|---|---|
| IND´bcp1 | Porcentaje de aplicaciones que cuentan con un plan de recuperación detallado.<br>Fórmula = X´bcp2*100/X´bcp1 |
| | |
| IND´bcp2 | Porcentaje de sistemas que cuentan con un plan de contingencia<br>Fórmula = X´bcp4*100/X´bcp3 |
| | |
| IND´bcp3 | Porcentaje de sistemas de gestión con planes de contingencias probados<br>Fórmula = X´bcp5*100/X´bcp3 |

| | |
|---|---|
| | |
| IND´bcp4 | Porcentaje de procesos de negocio que cuentan con un Plan de continuidad<br>Fórmula = X´bcp7*100/X´bcp6 |
| | |
| IND´bcp5 | Porcentaje de procesos de negocio con un BCP documentado.<br>Fórmula = X´bcp8*100/X´bcp6 |
| | |
| IND´bcp6 | Porcentaje de BCP de procesos de negocios que son auditados<br>Fórmula = X´bcp9*100/X´bcp7 |
| | |
| IND´bcp7 | Porcentaje de BCP de procesos de negocios que son actualizados.<br>Fórmula = Xbcp10*100/Xbcp7 |
| | |

## 5.5.- Resultados del proceso de política de seguridad.

Las variables son

| | |
|---|---|
| **X´pol1**<br>Frecuencia:<br>6 meses | Número de proveedores o de outsourcing con los que tiene relación la empresa<br>objetivo.- Determinar el número total de proveedores o outsourcing para poder establecer métricas |
| Con relación a Xpol5 | |
| **X´pol2**<br>Frecuencia:<br>6 meses | Número de proveedores o de outsourcing con los que se ha establecido una políticas de seguridad para el intercambio de información<br>Objetivo.- Determinar el % de proveedores o outsourcing con los que se han establecido políticas de seguridad. |
| Con relación a Xpol6 | |
| **X´pol3**<br>Frecuencia:<br>6 meses | Número de políticas corporativas totales que existen en la organización<br>Objetivo.- Determinar el número total de políticas corporativas que existen en una organización |
| Con relación a Xpol7 | |
| **X´pol4**<br>Frecuencia:<br>6 meses | Número de políticas especificas que han sido violadas por los usuarios<br>Objetivo.- Ayudará a determinar el % de políticas que han sido violadas |
| Con relación a Xpol8 | |
| **X´pol5**<br>Frecuencia: | Número de políticas que son actualizadas<br>Objetivo: Determinar una métrica del % de políticas Actualizadas |

| | |
|---|---|
| 1 año | |
| Con relación a Xpol9 | |
| **X´pol6**<br>Frecuencia:<br>1 año | Número de políticas que son auditadas<br>Objetivo: Determinar una métrica del % de políticas auditadas |
| Con relación a Xpol10 | |
| **X´pol7**<br>Frecuencia:<br>1 año | Número de políticas nuevas creadas<br>Objetivo.- Determinar el número de nuevas políticas creadas en un período de tiempo determinado |
| Con relación a Xpol11 | |

Las métricas que podemos construir a partir de estas variables son las siguientes.

| | |
|---|---|
| IND´pol1 | Porcentaje de proveedores o de outsourcing con los que se han desarrollado políticas de seguridad<br>Fórmula = X´pol2*100/X´pol1 |
| | |
| IND´pol2 | Porcentaje de políticas especificas que han sido violadas por los usuarios<br>Fórmula = X´pol4*100/X´pol3 |
| | |
| IND´pol3 | Porcentaje de políticas actualizadas<br>Fórmula = X´pol5*100/X´pol3 |
| | |
| IND´pol4 | Porcentaje de políticas que son auditadas<br>Fórmula = X´pol6*100/X´pol3 |
| | |
| IND´pol5 | Número de políticas nuevas creadas periódicamente<br>Fórmula = X´pol7 |
| | |

## 5.6.- Resultado del proceso equipo de respuesta a incidentes.

Las variables son

| | |
|---|---|
| **X´eri1**<br>Frecuencia:<br>Mensual | Número total de sistemas operativos de la organización que necesitan updates<br>Objetivo.-Determinar el número total de sistemas de la organización para poder determinar métricas |

| | |
|---|---|
| Con relación a Xeri1 | |
| **X´eri2**<br>Frecuencia:<br>Mensual | Número total de sistemas operativos que son actualizados<br>Objetivo.- Ayudará a determinar el porcentaje de sistemas que son actualizados |
| Con relación a Xeri2 | |
| **X´eri3**<br>Frecuencia:<br>6 meses | Costo total de daños que causaron los incidentes de seguridad<br>Objetivo.- Determina el costo total de daños para la empresa por los incidentes de seguridad |
| Con relación a Xeri3 | |
| **X´eri4**<br>Frecuencia:<br>6 meses | Número de incidentes que se resolvieron siguiendo procesos documentados.<br>Objetivo.- Ayudará a determinar una métrica del % de incidentes que se resuelven siguiendo procesos documentados |
| Con relación a Xeri4 | |
| **X´eri5**<br>Frecuencia:<br>1 año | Número de incidentes que ocurren en un tiempo determinado<br>Objetivo.- Con base a estadísticas determinar el número de incidentes que ocurren en un tiempo determinado |
| Con relación a Xeri5 | |
| **X´eri6**<br>Frecuencia:<br>1 año | Período de tiempo en que se cuantifica los incidentes<br>Objetivo.- Determinar un tiempo de monitoreo de incidentes puede ser cada 6 meses |
| Con relación a Xeri6 | |
| **X´eri7**<br>Frecuencia:<br>1 año | Número de incidentes de severidad 1 que ocurren en un período de 6 meses<br>Objetivo: Determinar el número de incidentes severidad 1 que ocurren en un período de tiempo determinado. |
| Con relación a Xeri7, Xeri8 y Xeri9 | |
| **X´eri8**<br>Frecuencia:<br>1 año | Número de incidentes de severidad 2 que ocurren en un período de 6 meses<br>Objetivo: Determinar el número de incidentes severidad 2 que ocurren en un período de tiempo determinado. |
| Con relación a Xeri7, Xeri8 y Xeri9 | |
| **X´eri9**<br>Frecuencia:<br>1 año | Número de incidentes de severidad 3 que ocurren en un período de 6 meses<br>Objetivo: Determinar el número de incidentes severidad 3 que ocurren en un período de tiempo determinado. |
| Con relación a Xeri7, Xeri8 y Xeri9 | |
| **X´eri10**<br>Frecuencia:<br>1 año | Número de incidentes de severidad 4 que ocurren en un período de 6 meses<br>Objetivo: Determinar el número de incidentes severidad 4 que ocurren en un período de tiempo determinado. |
| Con relación a Xeri7, Xeri8 y Xeri9 | |
| **X´eri11**<br>Frecuencia: | Número de incidentes resueltos en la primera llamada por help-desk en un período de 6 meses |

| | |
|---|---|
| 1 año | Objetivo: Determinar el porcentaje de incidentes que se resuelven por help-desk en la primera llamada |
| Con relación a Xeri10 | |
| **X´eri12**<br>Frecuencia:<br>1 año | Número de incidentes que se resuelven considerando desde que se detecta hasta que se lleva a una recuperación<br>Objetivo.- Determina el tiempo promedio en que se resuelve un incidente desde que se detecta hasta que se lleva a una recuperación que es lo mas importante, en este caso se considera que un incidente tiene 4 etapas: Análisis y Detección, Contención y erradicación, recuperación e investigación, revisión y seguimiento. |
| Con relación a Xeri11 | |
| **X´eri13**<br>Frecuencia:<br>1 año | Número de incidentes documentado(ataque llevados a la etapa de revisión y seguimiento) en un período de 6 meses<br>Objetivo: Determina el número de ataques que son documentados (llevados a la etapa de revisión y seguimiento) del total de incidentes ocurridos. |
| Con relación a Xeri12 | |
| **X´eri14**<br>Frecuencia:<br>1 año | Número de activos que cuentan con bitácora<br>Objetivo.- Determina el número de bitácoras que se pueden monitorear |
| Con relación a Xeri15 | |
| **X´eri15**<br>Frecuencia:<br>1 año | Número de activos que cuentan con respaldo<br>Objetivo.- Determina el número de activos que cuentan con un respaldo |
| Con relación a Xeri15 | |
| **X´eri16**<br>Frecuencia:<br>1 año | Número de activos con bitácora que cuentan con un control para la integridad de esta.<br>Objetivo.- Determina el número de activos con bitácora que cuentan con una medida de control para sus modificaciones, el fin es evitar que las bitácoras tengan un movimiento fuera de lo normal de sus modificaciones. |
| Con relación a Xeri116 | |
| **X´eri17**<br>Frecuencia:<br>1 año | Número de incidentes relacionados con espionaje en un período de 6 meses<br>Objetivo: Determina el número de ataques relacionados con espionaje que ocurren en un tiempo determinado |
| Con relación a Xeri17 | |
| **X´eri18**<br>Frecuencia:<br>1 año | Número de incidentes relacionados con (Hoax) en un período de 6 meses<br>Objetivo: Determina el número de ataques relacionados con (Hoax) que ocurren en un tiempo determinado |
| Con relación a Xeri17 | |
| **X´eri19**<br>Frecuencia:<br>1 año | Número de incidentes relacionados con código malicioso en un período de 6 meses<br>Objetivo: Determina el número de ataques relacionados con código malicioso(Este pude ser virus, spyware, adware, etc) |
| Con relación a Xeri17 | |

| | |
|---|---|
| **X´eri20**<br>Frecuencia:<br>1 año | Número de incidentes relacionados con probe en un período de 6 meses<br>Objetivo: Determina el número de ataques relacionados con probe que ocurren en un tiempo determinado |
| Con relación a Xeri17 | |
| **X´eri21**<br>Frecuencia:<br>1 año | Número de incidentes relacionados con acceso no autorizado/ cambios no autorizados en un período de 6 meses<br>Objetivo: Determina el número de accesos no autorizados/ cambios no autorizados que ocurren en un tiempo determinado |
| Con relación a Xeri18 | |
| **X´eri22**<br>Frecuencia:<br>1 año | Número de incidentes relacionados con uso no autorizado (misuse) en un período de 6 meses<br>Objetivo: Determina el número de ataques de uso no autorizado que ocurren en un tiempo determinado |
| Con relación a Xeri20 | |
| **X´eri23**<br>Frecuencia:<br>1 año | Número de incidentes relacionados con ataques de Spam en un período de 6 meses<br>Objetivo: Determina el número de ataques relacionados con Spam que ocurren en un tiempo determinado |
| Con relación a Xeri17 | |
| **X´eri24**<br>Frecuencia:<br>1 año | Número de actualizaciones al programa ERI en un período de 6 meses<br>Objetivo: Determina si se realizan actualizaciones al programa constantemente, estas actualizaciones pueden ser de algún tipo específico: modificación de procedimientos, acciones de mejora. |
| Con relación a Xeri22 | |

Algunos indicadores que podemos construir a partir de estas variables son los siguientes.

| Indicadores | Descripción. |
|---|---|
| IND´eri1 | Porcentaje total de sistemas operativos que son actualizados.<br>Fórmula = X´eri2*100/X´eri1 |
| | |
| IND´eril2 | Costo total de daños por incidentes para la organización<br>Fórmula = X´eri3 |
| | |
| IND´eri3 | Porcentaje de incidentes que se resuelven siguiendo procesos documentados<br>Fórmula = X´eri4*100/X´eri5 |
| | |
| IND´eri4 | Porcentaje de incidentes de severidad 1 que ocurren en un tiempo determinado. |

| | |
|---|---|
| | Fórmula = (X´eri7*100)/X´eri5 |
| | |
| IND´eri5 | Porcentaje de incidentes de severidad 2 que ocurren en un tiempo determinado.<br>Fórmula = (X´eri8*100)/X´eri5 |
| | |
| IND´eri6 | Porcentaje de incidentes de Severidad 3 que ocurren en un tiempo determinado.<br>Fórmula = (X´eri9*100)/X´eri5 |
| | |
| IND´eri7 | Porcentaje de incidentes de Severidad 4 que ocurren en un tiempo determinado.<br>Fórmula = (X´eri10*100)/X´eri5 |
| | |
| IND´eri8 | Porcentaje de incidentes que se resuelven por help-desk en la primera llamada en un período de 6 meses<br>Fórmula = X´eri11*100/X´eri5 |
| | |
| IND´eri9 | Porcentaje de incidentes documentados periódicamente<br>Fórmula = (X´eri13*100)/X´eri5 |
| | |
| IND´eri10 | Porcentaje de incidentes resueltos periódicamente<br>Fórmula = (Xeri12*100)/Xeri1 |
| | |
| IND´eri11 | Porcentaje de incidentes no resueltos periódicamente<br>Fórmula = (X´eri5 – X´eri12) |
| | |
| IND´eri12 | Porcentaje de activos que cuentan con bitácoras<br>Fórmula = (X´eri14*100) / Número total de activos de la organización |
| | |
| IND´eri13 | Porcentaje de activos que cuentan con respaldo<br>Fórmula = (X´eri15*100)/ Número total de activos de la organización. |
| | |

| | |
|---|---|
| IND´eri14 | Porcentaje de activos con bitácora que cuentan con un control para la integridad de esta.<br>Fórmula = (X´eri16*100)/X´eri14 |
| | |
| IND´eri15 | porcentaje de incidentes de relacionados con espionaje periódicamente.<br>Fórmula = Xeri17*100/X´eri5 |
| | |
| IND´eri16 | Porcentaje de incidentes relacionados con Hoax periódicamente.<br>Fórmula = X´eri18*100/X´eri5 |
| | |
| IND´eri17 | Porcentaje de incidentes relacionados con código malicioso periodicamente<br>Fórmula = X´eri19*100/X´eri5 |
| | |
| IND´eri18 | Porcentaje de incidentes relacionados con probe periódicamente.<br>Fórmula = X´eri20*100/X´eri5 |
| | |
| IND´eri19 | Porcentaje de incidentes relacionados con acceso no autorizados/cambios no autorizados periódicamente.<br>Fórmula = X´eri21*100/X´eri5 |
| | |
| IND´eri20 | Porcentaje de incidentes relacionados con uso no autorizado (misuse) en un período de 6 meses<br>Fórmula = X´eri22*100/X´eri5 |
| | |
| IND´eri21 | Porcentaje de incidentes relacionados con ataques de Spam en un período de 6 meses<br>Fórmula = X´eri23*100/X´eri5 |
| | |
| IND´eri22 | Número de actualizaciones al programa ERI periódicas<br>Fórmula = X´eri24 |
| | |

## 5.7.- Resultado del proceso Control de accesos.

Las variables son

| | |
|---|---|
| **X´ca1**<br>Frecuencia:<br>1 año | Número total de sistemas con que cuenta la organización en un período de 1 año<br>Objetivo.- Determinar el número total de sistemas con que cuenta la organización para poder realizar métricas. |
| Con relación a Xca1 | |
| **X´ca2**<br>Frecuencia:<br>1 año | Número total de controles en los sistemas que requieren ser implementados<br>Objetivo.- Determinar el número total de controles en los sistemas que requieren ser implementados dentro de la organización. |
| Con relación a Xca3 | |
| **X´ca3**<br>Frecuencia:<br>1 año | Número total de controles en los sistemas que son implementados.<br>Objetivo.- Determinar el número del total de controles que fueron implementados en un período de tiempo determinado. |
| Con relación a Xca3 | |
| **X´ca4**<br>Frecuencia:<br>1 año | Número de sistemas que cuentan con controles TECNICOS desde su implementación<br>Objetivo.- Determinar el número total de sistemas que cuentan con controles técnicos desde su implementación, estos controles deben estar previamente definidos. |
| Con relación a Xca3 | |
| **X´ca5**<br>Frecuencia:<br>1 año | Número de sistemas que han modificado sus controles TECNICOS desde su implementación<br>Objetivo.- Construir una métrica con el número de sistemas que han modificado sus controles técnicos desde su implementación |
| Con relación a Xca4 | |
| **X´ca6**<br>Frecuencia:<br>1 año | Número de usuarios con accesos especiales a sistemas en un período de 1 año<br>Objetivo.- Determinar el número total de usuarios con accesos especiales para definir métricas, estos permisos especiales pueden ser: dar un permiso especial a una persona en determinada aplicación a la cual regularmente no tiene acceso pero lo necesita por algún proyecto especial o también permitirle instalar una aplicación que esta prohibida en la empresa. |
| Con relación a Xca5 | |
| **X´ca7**<br>Frecuencia:<br>1 año | Número total de usuarios con accesos especiales que han sido auditados en un período de 1 año<br>Objetivo.- Determinar si los usuarios con accesos especiales representan una amenaza |
| Fuente: Corporate information security working group | |
| **X´ca8**<br>Frecuencia:<br>1 año | Número total de líneas o enlaces de entradas con los que cuenta la organización.<br>Objetivo.- Determinar el número total de líneas o enlaces de entrada con los que cuenta la organización para construir una métrica de medición. |
| Con relación a Xca9 | |

| | |
|---|---|
| **X´ca9**<br>Frecuencia:<br>1 año | Número total de líneas o enlaces de entrada dentro de la organización que cuentan con restricciones de acceso para todos sus puntos de entrada<br>objetivo.- Determinar una métrica del porcentaje total de líneas o enlaces de entrada que cuentan con restricciones de acceso |
| Con relación a Xca9 | |
| **X´ca10**<br>Frecuencia:<br>1 año | Número total de PCS en la organización<br>Objetivo.- Determinar el número total de PCS con que cuenta la organización(debe definirse un estándar de encriptación) |
| Con relación a Xca11 | |
| **X´ca11**<br>Frecuencia:<br>1 año | Número total de PCS que cuentan con capacidad de encriptación para sus archivos<br>Objetivo.- Construir una métrica que determine el porcentaje de PCS con capacidad de encriptación. |
| Con relación a Xca12 | |
| **X´ca12**<br>Frecuencia:<br>6 meses | Número total de sistemas con restricciones para el personal de mantenimiento(el tipo de restricciones deben estar definidas)<br>Objetivo.- Determinar una métrica que busque reducir el nivel de riesgo de modificaciones a sistemas por personal de mantenimiento. |
| Con relación a Xca13 | |
| **X´ca13**<br>Frecuencia<br>1 mes | Número de aplicaciones que requieren updates<br>objetivo.- Determinar el número total de aplicaciones que requieren actualizaciones |
| Con relación a Xca16 | |
| **X´ca14**<br>Frecuencia:<br>1 mes | Número de aplicaciones que se les aplicaron todas las actualizaciones en un período de un mes<br>Objetivo.- Determinar una métrica de porcentaje del número de aplicaciones que se les instalaron todas sus actualizaciones. |
| Con relación a Xca17 | |
| **X´ca15**<br>Frecuencia:<br>1 año | Número total de sistemas que cambiaron el password que traen del fabricante<br>Objetivo.- Determinar una métrica que ayude a minimizar los accesos no autorizados |
| Con relación a Xca18 | |
| **X´ca16**<br>Frecuencia:<br>1 año | Número total de sistemas que corren protocolos restringidos (estos protocolos deben estar definidos con anterioridad).<br>Objetivo.- Ayudará a determinar una métrica para el % de sistemas que corren protocolos restringidos. |
| Con relación a Xca19 | |

Algunos indicadores que podemos construir a partir de variables son los siguientes.

| Indicadores | Descripción. |
|---|---|
| IND´ca1 | Porcentaje total de controles en los sistemas que son implementados en un período de 1 año<br>Fórmula = X´ca3*100/X´ca2 |
| | |
| IND´cal2 | Porcentaje de sistemas que cuentan con controles TECNICOS desde su implementación<br>Fórmula = X´ca4*100/X´ca1 |
| | |
| IND´ca3 | Porcentaje de usuarios con accesos especiales a sistemas que han sido auditados en un período de 1 año<br>Fórmula = X´ca7*100/X´ca6 |
| | |
| IND´ca4 | Porcentaje total de líneas o enlaces en la organización que cuentan con restricción de accesos<br>Fórmula = X´ca9*100/X´ca8 |
| | |
| IND´ca5 | Porcentaje de PCS con capacidad de encriptación<br>Fórmula = X´ca11*100/X´ca10 |
| | |
| IND´ca6 | Porcentaje de sistemas con restricciones al personal de acceso<br>Fórmula = X´ca12*100/X´ca1 |
| | |
| IND´ca7 | Porcentaje de aplicaciones que recibieron todas sus actualizaciones en un período de 1 mes<br>Fórmula = X´ca14*100/X´ca13 |
| | |
| IND´ca8 | Porcentaje de sistemas que cambiaron el password del fabricante Fórmula = X´ca15*100/X´ca1 |
| | |
| IND´ca9 | Porcentaje de sistemas que corren protocolos restringidos<br>Fórmula = X´ca16*100/X´ca1 |
| | |

## 5.8.- Resultado del proceso Análisis de riesgos.

Las variables son

| Variables | Descripción. |
|---|---|
| **X´irm1**<br>Frecuencia:<br>1 año | Número total de activos con los que cuenta la empresa<br>Objetivo.- Determinar el número total de activos con los que cuenta la empresa (estos pueden ser dispositivos, aplicaciones, datos, información en papel, etc.) |
| Con relación a Xirm1 | |
| **X´irm2**<br>Frecuencia:<br>1 año | Número de activos a los que se les aplico un IRM en un período de 1 año<br>Objetivo.- Conocer el número total de activos que se les aplica un IRM |
| Con relación a Xirm1 | |
| **X´irm3**<br>Frecuencia:<br>3 meses | Número de riesgos (del total de activos) que son aceptados y que no les ha expirado la fecha de aceptación (se utilizó carta de aceptación de riesgos)<br>Objetivo: Determinar el número total de riesgos que fueron aceptados y que no les ha expirado la fecha de aceptación |
| Con relación a Xirm4 | |
| **X´irm4**<br>Frecuencia:<br>3 meses | Número de riesgos (del total de sistemas) que son aceptados y que les expiró la fecha de aceptación<br>Objetivo: Determinar el número total de riesgos que fueron aceptados y que ya les expiró la fecha de aceptación |
| Con relación a Xirm4 | |
| **X´irm5**<br>Frecuencia:<br>1 año | Número de riesgos mitigados vs. No mitigados en un período de 1 año<br>Objetivo.- Determinar el número de riesgos mitigados vs. no mitigados en un período de 1 año |
| Con relación a Xirm5 | |
| **X´irm6**<br>Frecuencia:<br>3 meses | Número de riesgos altos y medios no mitigados por activo<br>Objetivo: Determinar el número total de riesgos altos y medios no mitigados por activo |
| Con relación a Xirm6 | |
| **X´irm7**<br>Frecuencia:<br>3 meses | Número de controles no implementados por activo<br>Objetivo: Determinar el número total de controles no implementados por activo |
| Con relación a Xirm6 | |
| **X´irm8**<br>Frecuencia:<br>3 meses | Número de vulnerabilidades o debilidades críticas descubiertas por activo.<br>Objetivo.- Conocer el total de vulnerabilidades críticas por activo |
| Con relación a Xirm6 | |
| **X´irm9**<br>Frecuencia:<br>3 meses | Número de vulnerabilidades críticas reparadas vs. no reparadas por activo<br>Objetivo.- Conocer el total de vulnerabilidades críticas vs. no críticas por activo, conocer el tiempo promedio de reparación y de no reparación de vulnerabilidades críticas |

| | |
|---|---|
| Con relación a Xirm6 | |
| **X´irm10**<br>Frecuencia:<br>1 año | Número de sistemas con IRM que son revisados por dirección general en un período de 1 año<br>Objetivo.- Determinar el grado de involucramiento de la dirección |
| Con relación a Xirm7 | |
| **X´irm11**<br>Frecuencia:<br>1 año | Número de activos críticos para los cuales el costo por daño o perdida ha sido cuantificado en un período de 1 año<br>Objetivo.- Determinar el número de activos totales cuyo costo por daño o perdida ha sido cuantificado |
| Con relación a Xirm8 | |
| **X´irm12**<br>Frecuencia:<br>1 año | Número de riesgos que están relacionados con amenazas externas en un período de un 1 año<br>Objetivo.- Ayudará a determinar el porcentaje de amenazas externas |
| Con relación a Xirm9 | |
| **X´irm13**<br>Frecuencia:<br>1 año | Número de nuevas vulnerabilidades que se les da seguimiento desde el último reporte<br>Objetivo.- Determinar el número total de vulnerabilidades que se les da seguimiento desde el último reporte |
| Con relación a Xirm10 | |

Algunas de las métricas que podemos construir a partir de estas variables son las siguientes.

| Indicadores | Descripción. |
|---|---|
| IND´irm1 | Porcentaje de activos que se les aplico un IRM en un período de 1 año<br>Fórmula = (X´irm2*100)/X´irm1 |
| | |
| IND´irm2 | Porcentaje de riesgos (del total de activos) que son aceptados y que no les ha expirado la fecha de aceptación (se utilizó carta de aceptación de riesgos)<br>Fórmula = (X´irm3*100/X´irm1 |
| | |
| IND´irm3 | Porcentaje de riesgos (del total de sistemas) que son aceptados y que les expiró la fecha de aceptación<br>Fórmula = X´irm4*100/X´irm1 |
| | |
| IND´irm4 | Porcentaje de riesgos mitigados en un período de 1 año<br>Fórmula = X´irm5*100/total de riesgos detectados en un año |
| | |

| | |
|---|---|
| IND´irm6 | Número de riesgos de altos y medios no mitigados por activos.<br>Fórmula = X´irm6 |
| | |
| IND´irm7 | Número de controles no implementados por activo<br>Fórmula = X´irm7 |
| | |
| IND´irm8 | Número de vulnerabilidades o debilidades críticas descubiertas por activo.<br>Fórmula = X´irm8 |
| | |
| IND´irm9 | Porcentaje de sistemas con IRM revisados por dirección en un período de 1 año<br>Fórmula = X´irm10*100/X´irm2 |
| | |
| IND´irm10 | Porcentaje de activos cuyo costo por daño o perdida ha sido cuantificado<br>Fórmula = X´irm11*100 / Número total de activos |
| | |
| IND´irm11 | Porcentaje de riesgos externos en un período de 1 año<br>Fórmula = X´irm12*100/ Número de riesgos detectados en un período de 1 año |
| | |
| IND´irm12 | Número de nuevas vulnerabilidades descubiertas desde el último reporte<br>Fórmula = X´irm13 |
| | |

## 5.9.- Matriz de resultados

Como se menciono anteriormente, de las variables propuestas solo se utilizaron algunas, otras se modificaron y algunas otras fueron eliminadas. A continuación se muestra un cuadro con estos resultados.

Tabla 11.- Matriz de resultados

| **PROCESO CONCIENTIZACIÓN,** | | | |
|---|---|---|---|
| Variables Generales | Variables Utilizadas | Variables eliminadas | Observaciones |
| **Xcon1.-** Número de empleados Totales de la organización. | **X´con1.-** Número de empleados Totales de la organización. | | |
| **Xcon2.-** Período de tiempo en que se realizan las revisiones o auditorias al proceso de concientización en promedio será 6 meses. | **X´con2.-** Período de tiempo en que se realizan las revisiones o auditorias al proceso de concientizacion en promedio será 6 meses | | |
| **Xcon3.-** Número de empleados que reciben capacitación sobre concientización en un período de 6 meses. | **X´con3.-** Número de empleados que reciben capacitación sobre concientizacion en un período de 6 meses | | |
| **Xcon4.-** Número de Actividades de concientización que se realizan en un período de 6 meses. | | **Xcon4** | Esta variable fue eliminada debido a que en esta empresa existen varios tipos de actividades |
| **Xcon5.-** Número de audiencias creadas para las diferentes actividades de concientización en un período de 6 meses. | **X´con5.-** Número de audiencias creadas para las diferentes actividades de concientizacion en un período de 6 meses | | |
| **Xcon6.-** Número de empleados que asisten por audiencia en un período de 6 meses. | **X´con6.-** Número total de personas por audiencia que ya recibió capacitación customizada para el | | |

| | | | |
|---|---|---|---|
| | grupo de audiencia al cual pertenece. | | |
| **Xcon7.-** Número total de tópicos que buscan revisarse en las actividades de concientización. | **X´con7.-** Número total de tópicos que buscan revisarse en las actividades de concientizacion. | | |
| **Xcon8.-** Número de tópicos que realmente se ven en las actividades de concientización. | **X´con8.-** Número de tópicos que realmente se ven en las actividades de concientizacion | | |
| **Xcon9.-** Número de actividades de concientización a las que asiste un empleado en un período de 6 meses. | **X´con9.-** número de actividades de concientizacion a las que asiste un empleado en un período de 6 meses | | |
| **Xcon10.-** Total de horas que dura un empleado en entrenamiento en un período de 6 meses | **X´con10.-** Número total de empleados que asisten a más horas de entrenamiento en actividades de concientizacion. | | |
| **Xcon11.-** Número total de empleados que asisten a mas horas de entrenamiento en actividades de concientización | | **Xcon11** | La empresa no considera necesario saber el total de horas que un empleado pasa en actividades de concientización, es mejor saber si acredita los cursos. |
| **Xcon12.-** Número de empleados que presentan las encuestas y exámenes de concientización en un período de 6 meses | **X´con4.-** Número de empleados que recibe una constancia de acreditación al final de una sesión de entrenamiento. | | |
| **Xcon13.-** Número de empleados que contestan correctamente las | | **Xcon13** | El objetivo en esta variable esta contenido en X´con4. |

| | | | |
|---|---|---|---|
| encuestas de concientización en un período de 6 meses | | | |
| **Xcon14.-** Número de reportes de incidentes levantados en un período de 6 meses | **X´con11.-** Número de reportes de incidentes levantados en un período de 6 meses | | |
| **Xcon15.-** Número de personas que han tomado cursos de concientización y que levantaron reporte de incidentes en un período de 6 meses | | **Xcon15** | El objetivo es algo secundario, ya esta definido dentro de X´con11. |
| | | | |
| **PROCESO BCM** | **En este caso todas las variables fueron utilizadas.** | | |
| Variables Generales | Variables Utilizadas | Variables eliminadas | Observaciones |
| **Xbcp1.-** Número de total de aplicaciones críticas que requieren respaldo | **X´bcp1.-** Número de total de procesos de negocio dentro de la organización. | | |
| **Xbcp2.-** Número total de aplicaciones críticas que son respaldados frecuentemente de acuerdo a la norma | **X´bcp2.-** Número total de procesos de negocio que cuentan con un plan de recuperación detallado. | | |
| **Xbcp3.-** Número de total de sistemas de la organización | **X´bcp3.-** Número total de sistemas de la organización | | |
| **Xbcp4.-** Número total de sistemas que cuentan con un plan de contingencia. | **X´bcp4.-** Número total de sistemas que cuentan con un plan de contingencia. | | |
| **Xbcp5-** Número de total de sistemas de gestión de negocio que tienen planes de contingencia probados | **X´bcp5.-** Número total de sistemas gestión de negocio que tienen planes de contingencia probados | | |
| **Xbcp6.-** Número total de unidades organizacionales | **X´bcp6.-** Número total procesos de negocios dentro de la organización. | | En lugar de utilizar unidades de negocio se enfoca a procesos de |

| | | | |
|---|---|---|---|
| | | | negocio. |
| **Xbcp7.-** Número de total de unidades organizacionales que cuentan con un plan de continuidad | **X´bcp7.-** Número total de procesos de negocio que cuentan con un plan de continuidad | | En lugar de utilizar unidades de negocio se enfoca a procesos de negocio. |
| **Xbcp8.-** Número total de unidades organizacionales que cuentan con un plan de continuidad documentado. | **X´bcp8.-** Número total de procesos de negocio que cuentan con un plan de continuidad documentado. | | En lugar de utilizar unidades de negocio se enfoca a procesos de negocio. |
| **Xbcp9.-** Número de total de planes de BCP de unidades de negocios que son auditados | **X´bcp9.-** Número total de planes de BCP de procesos de negocio que son auditados | | |
| **Xbcp10.-** Número total de planes de BCP de unidades de negocios que son actualizados | **X´bcp10.-** Número total de planes de BCP de procesos de negocio que son auditados | | |
| | | | |
| **PROCESO DE POLITICA** | | | |
| Variables Generales | Variables Utilizadas | Variables eliminadas | Observaciones |
| **Xpol1.-** Número de total de sistemas con passwords | | **Xpol1** | Esta variable es más de implementación no de política. |
| **Xpol2.-** Número total de sistemas que cuentan con política de password | | **Xpol2** | Esta variable es más de implementación no de política. |
| **Xpol3.-** Número de total de websites con los que cuenta la organización | | **Xpol3** | Esta variable es más de implementación no de política. |
| **Xpol4.-** Número total de websites que cuentan con política de seguridad incorporada | | **Xpol4** | Esta variable es más de implementación no de política. |
| **Xpol5.-** Número de proveedores o de | **X´pol1.-** Número de proveedores o de | | |

| | | | |
|---|---|---|---|
| outsourcing con los que tiene relación la empresa | outsourcing con los que tiene relación la empresa | | |
| **Xpol6.-** Número de proveedores o de outsourcing con los que se ha establecido una políticas de seguridad para el intercambio de información | **X´pol2.-** Número de proveedores o de outsourcing con los que se ha establecido una políticas de seguridad para el intercambio de información | | |
| **Xpol7.-** Número de políticas corporativas totales que existen en la organización | **X´pol3.-** Número de políticas corporativas totales que existen en la organización | | |
| **Xpol8.-** Número de políticas especificas que han sido violadas por los usuarios | **X´pol4.-** Número de políticas especificas que han sido violadas por los usuarios | | |
| **Xpol9.-** Número de políticas que son actualizadas | **X´pol5.-** Número de políticas que son actualizadas | | Se cambio el periodo a 1 o 2 años. |
| **Xpol10.-** Número de políticas que son auditadas | **X´pol6.-** Número de políticas que son auditadas | | Se cambio el periodo a 1 o 2 años. |
| **Xpol11.-** Número de políticas nuevas creadas | **X´pol7.-** Número de políticas nuevas creadas | | |
| **Xpol12.-** Número de aplicaciones que cuentan con procedimiento de respaldo en la organización | | **Xpol12** | Esta variable es más de implementación no de política. |
| **Xpol13.-** Número de aplicaciones cuyo respaldos se realizan de acuerdo a la política de respaldo | | **Xpol13** | Esta variable es más de implementación no de política. |
| | | | |
| **PROCESO DE ERI** | | | |
| Variables Generales | Variables Utilizadas | Variables eliminadas | Observaciones |
| **Xeri1.-** Número de total de sistemas operativos de la | **X´eri1.-** Número total de sistemas operativos de la | | |

| | | | |
|---|---|---|---|
| organización que necesitan updates | organización que necesitan updates | | |
| **Xeri2.-** Número total de sistemas operativos que se les instala sus updates frecuentemente | **X´eri2.-** Número total de sistemas operativos que son actualizados | | Se puede manejar como sistemas operativos actualizados. |
| **Xeri3.-** Costo total de daños que causaron los incidentes de seguridad | **X´eri3.-** Costo total de daños que causaron los incidentes de seguridad | | |
| **Xeri4.-** Número de incidentes que se resolvieron siguiendo procesos documentados | **X´eri4.-** Número de incidentes que se resolvieron siguiendo procesos documentados. | | |
| **Xeri5.-** Número de incidentes que ocurren en tiempo determinado | **X´eri5.-** Número de incidentes que ocurren en un tiempo determinado | | |
| **Xeri6.-** Tiempo en que se revisan los incidentes puede ser 6 meses | **X´eri6.-** Período de tiempo en que se cuantifica los incidentes | | |
| **Xeri7.-** Número de incidentes graves en un período de 6 meses | **X´eri7.-** Número de incidentes de severidad 1 que ocurren en un período de 6 meses | | Se utilizo incidentes de severidad 1, en lugar de alta gravedad |
| **Xeri8.-** Número de incidentes de gravedad media en un período de 6 meses | **X´eri8.-** Número de incidentes de severidad 2 que ocurren en un período de 6 meses | | Se utilizo incidentes de severidad 2, en lugar de gravedad media. |
| **Xeri9.-** Número de incidentes de baja gravedad en un período de 6 meses | **X´eri9.-** Número de incidentes de severidad 3 que ocurren en un período de 6 meses<br>**X´eri10.-** Número de incidentes de severidad 4 que ocurren en un período de 6 meses | | De la variable Xeri9 se definieron dos métricas que corresponden a severidad 3 y 4. |
| **Xeri10.-** Número de incidentes resueltos en | **X´eri11.-** Número de incidentes resueltos | | |

| | | | |
|---|---|---|---|
| la primera llamada por help-desk en un período de 6 meses | en la primera llamada por help-desk en un período de 6 meses | | |
| **Xeri11.-** Tiempo de respuesta en el que se resuelve un incidente desde que se detecta hasta que se soluciona | **X´eri12.-** Número de incidentes que se resuelven considerando desde que se detecta hasta que se lleva a una recuperación | | |
| **Xeri12.-** Número de incidentes de ataques documentados en un período de 6 meses | **X´eri13.-** Número de incidentes documentado(ataque llevados a la etapa de revisión y seguimiento) en un período de 6 meses | | |
| **Xeri13.-** Número de incidentes resueltos exitosamente en un período de 6 meses | | **Xeri13** | Ya esta considerado dentro X´eri12. |
| **Xeri14.-** Número de incidentes que no son resueltos exitosamente en un período de 6 meses | | **Xeri14** | Ya esta considerado dentro X´eri12. |
| **Xeri15.-** Número de activos que cuentan con bitácora | **X´eri14.-** Número de activos que cuentan con bitácora<br>**X´eri15.-** Número de activos que cuentan con respaldo | | Con esta variable se construyeron dos métricas. |
| **Xeri16.-** Número de activos que sufren modificaciones en sus bitácoras | **X´eri16.-** Número de activos con bitácora que cuentan con un control para la integridad de esta. | | |
| **Xeri17.-** Número de incidentes de virus, spyware y adware detectados en un período de 6 meses | **X´17.-** Número de incidentes relacionados con espionaje en un período de 6 meses<br>**X´eri18.-** Número de incidentes relacionados con (Hoax) en un período | | Con esta variable se definieron 4 variables diferentes, cada una hace referencia a un tipo de código malicioso. |

| | | | |
|---|---|---|---|
| | de 6 meses<br>**X´eri19.-** Número de incidentes relacionados con código malicioso en un período de 6 meses<br>**X´eri20.-** Número de incidentes relacionados con probe en un período de 6 meses<br>**X´eri23.-** Número de incidentes relacionados con ataques de Spam en un período de 6 meses | | |
| **Xeri18.-** Número de incidentes de intrusiones por sistema o aplicación en un período de 6 meses | **X´eri21.-** Número de incidentes relacionados con acceso no autorizado/ cambios no autorizados en un período de 6 meses | | |
| **Xeri19.-** Número de incidentes de ataques a los firewalls en un período de 6 meses | | **Xeri9** | Tendría que definirse que tipo de ataques. |
| **Xeri20.-** Número de incidentes de usos no autorizados en un período de 6 meses | **X´eri22.-** Número de incidentes relacionados con uso no autorizado (misuse) en un período de 6 meses | | |
| **Xeri21.-** Número de aplicaciones o programas no autorizados en la empresa en un período de 6 meses | | **Xeri21** | Es de poca utilidad para la empresa |
| **Xeri22.-** Número de actualizaciones al programa ERI en un período de 6 meses | **X´eri24.-** Número de actualizaciones al programa ERI en un período de 6 meses | | |
| | | | |

| **PROCESO DE CONTROL DE ACCESOS** | | | |
|---|---|---|---|
| Variables Generales | Variables Utilizadas | Variables eliminadas | Observaciones |
| **Xca1.-** Número de total de sistemas con que cuenta la organización en un período de 1 año | **X´ca1.-** Número total de sistemas con que cuenta la organización en un período de 1 año | | |
| **Xca2.-** Número de sistemas con controles Técnicos probados en un período de 1 año | | **Xca2** | Tendría que definirse que tipo controles técnicos, la empresa maneja varios tipos. |
| **Xca3.-** Número de sistemas que cuentan con controles TECNICOS desde su implementación | **X´ca2.-** Número total de controles en los sistemas que requieren ser implementados<br>**X´ca3.-** Número total de controles en los sistemas que son implementados.<br>**X´ca4.-** Número de sistemas que cuentan con controles TECNICOS desde su implementación | | De esta variable se definieron 3 diferentes que tienen que ver con los controles. |
| **Xca4.-** Número de sistemas que han modificado sus controles TECNICOS desde su implementación | **X´ca5.-** Número de sistemas que han modificado sus controles TECNICOS desde su implementación | | |
| **Xca5.-** Número de usuarios con accesos especiales a sistemas en un período de 1 año | **X´ca6.-** Número de usuarios con accesos especiales a sistemas en un período de 1 año | | |
| **Xca6.-** Número total de usuarios con accesos especiales que han sido auditados en un período de 1 año | **X´ca7.-** Número total de usuarios con accesos especiales que han sido auditados en un | | |

| | | | |
|---|---|---|---|
| | período de 1 año | | |
| **Xca7.-** Número total de contenedores de medios de respaldo | | **Xca7** | No relaciona la empresa esta variable con el control de accesos. |
| **Xca8.-** Número total de contenedores de respaldo que cuentan con logs de deposito y retiro de respaldos | | **Xca8** | No relaciona la empresa esta variable con el control de accesos. |
| **Xca9.-** Número total de de instalaciones de telecomunicaciones que cuentan con líneas de transmisión de datos | **X´ca8.-** Número total de líneas o enlaces de entradas con los que cuenta la organización. **X´ca9.-** Número total de líneas o enlaces de entrada dentro de la organización que cuentan con restricciones de acceso para todos sus puntos de entrada | | |
| **Xca10.-** Número total de instalaciones de telecomunicaciones que cuentan con restricciones de acceso | | **Xca10** | En esta variable tendría que definirse que tipo de restricciones de acceso. |
| **Xca11.-** Número total de PCS en la organización | **X´ca10.-** Número total de PCS en la organización | | |
| **Xca12.-** Número total de PCS que cuentan con capacidad de encriptación para sus archivos | **X´ca11.-** Número total de PCS que cuentan con capacidad de encriptación para sus archivos | | |
| **Xca13.-** Número total de sistemas con restricciones para el personal de mantenimiento | **X´ca12.-** Número total de sistemas con restricciones para el personal de mantenimiento(el tipo de restricciones deben estar | | |

| | | | |
|---|---|---|---|
| | definidas) | | |
| **Xca14.-** Número total de de modificaciones de software en un periodo de 1 año | | **Xca14** | No relaciona la empresa esta variable con el control de accesos. |
| **Xca15.-** Número total de modificaciones de software Documentados | | **Xca15** | No relaciona la empresa esta variable con el control de accesos. |
| **Xca16.-** Número de aplicaciones que requieren updates | **X´ca13.-** Número de aplicaciones que requieren updates | | |
| **Xca17.-** Número de aplicaciones que se les aplicaron todas las actualizaciones en un periodo de un mes | **X´ca14.-** Número de aplicaciones que se les aplicaron todas las actualizaciones en un período de un mes | | |
| **Xca18.-** Número total de sistemas que cambiaron el password que traen del fabricante | **X´ca15.-** Número total de sistemas que cambiaron el password que traen del fabricante | | |
| **Xca19.-** Número total de sistemas que corren protocolos restringidos. | **X´ca16.-** Número total de sistemas que corren protocolos restringidos (estos protocolos deben estar definidos con anterioridad). | | |
| | | | |
| **PROCESO DE ANALISIS DE RIESGOS** | | | |
| Variables Generales | Variables Utilizadas | Variables eliminadas | Observaciones |
| **Xirm1.-** Número total de sistemas con los que cuenta la empresa | **X´irm1.-** Número total de activos con los que cuenta la empresa<br>**X´irm2.-** Número de activos a los que se les aplico un IRM en un período de 1 año | | De Xirm1 se definieron dos variables diferentes. |
| **Xirm2.-** Número de | | **Xirm2** | Ya se definieron |

| | | | |
|---|---|---|---|
| sistemas que se les aplica un IRM en un período de 1 año | | | correctamente dentro de X´irm1 y X´irm2. |
| **Xirm3.-** Número de sistemas que cuentan con IRM documentado en un período de 1 año | | **Xirm3** | Ya se definieron correctamente dentro de X´irm1 y X´irm2. |
| **Xirm4.-** Número de riesgos del total de sistemas, que son aceptados y no se les da seguimiento | **X´irm3.-** Número de riesgos (del total de activos) que son aceptados y que no les ha expirado la fecha de aceptación (se utilizó carta de aceptación de riesgos)<br>**X´irm4.-** Número de riesgos (del total de sistemas) que son aceptados y que les expiró la fecha de aceptación | | De Xirm4 se definieron dos variables diferentes. |
| **Xirm5.-** Número de riesgos mitigados en un período de 1 año | **X´irm5.-** Número de riesgos mitigados vs. No mitigados en un período de 1 año | | |
| **Xirm6.-** Número de vulnerabilidades o debilidades descubiertas en un período de 1 año | **X´irm6.-** Número de riesgos altos y medios no mitigados por activo<br>**X´irm7.-** Número de controles no implementados por activo<br>**X´irm8.-** Número de vulnerabilidades o debilidades críticas descubiertas por activo.<br>**X´irm9.-** Número de vulnerabilidades críticas reparadas vs. no reparadas por activo | | A partir de Xirm6 se definieron 4 variables diferentes |
| **Xirm7.-** Número de sistemas con IRM que | **X´irm10.-** Número de sistemas con IRM | | |

| | | | |
|---|---|---|---|
| son revisados por dirección general en un período de 1 año | que son revisados por dirección general en un período de 1 año | | |
| **Xirm8.-** Número de activos críticos para los cuales el costo por daño perdida ha sido cuantificado en un período de 1 año | **X´irm11.-** Número de activos críticos para los cuales el costo por daño o perdida ha sido cuantificado en un período de 1 año | | |
| **Xirm9.-** Número de riesgos que están relacionados con amenazas externas en un período de un 1 año | **X´irm12.-** Número de riesgos que están relacionados con amenazas externas en un período de un 1 año | | |
| **Xirm10.-** Número de nuevas vulnerabilidades que se les da seguimiento desde el último reporte | **X´irm13.-** Número de nuevas vulnerabilidades que se les da seguimiento desde el último reporte | | |

## 5.10.- Conclusiones caso.

En general la mayoría de variables quedo expresada en su forma original, aunque en muchas otras tuvieron que adaptarse a la metodología de los procesos de la empresa, como mencionamos anteriormente algunas variables no se tomaron en cuenta pero estas dieron pie a la creación de nuevas variables.

El conjunto de variables generales obtenidos puede ser utilizado por cualquier empresa y adaptado a la forma en que realice sus procesos, sin embargo mientras menos estandarizados tenga sus procesos, será mas difícil plantear un modelo de seguridad de información confiable.

De aquí podemos concluir que es muy importante que los procesos estén desarrollados en base a mejores practicas y además siguiendo metodologías y estándares adecuados.

# Capitulo 6.- Aportación.

## *Aportación personal.*

### 6.1.-Aportación

Durante la investigación de los procesos en lo personal pude identificar algunas variables que serian de interés, estas variables se tomaron en cuenta ya que atendían cierta parte del proceso que era importante estar monitoreando. Lo mismo sucedió con algunos indicadores.

La lista de variables e indicadores aportados se lista a continuación, también se mencionan las fuentes, es decir documentos que se analizaron y se consideraron para la creación de estas variables.

Tabla 12.- Variables e indicadores aportados

**Proceso concientización**

| Variables | Descripción. |
|---|---|
| **Xcon5**<br>Frecuencia:<br>6 Meses | Número de audiencias creadas para las diferentes actividades de concientización en un período de 6 meses.<br>Objetivo.- Determina si se han creado suficientes números de audiencias para cubrir las necesidades específicas en determinados tipos de empleados. |
| Fuentes de referencia: Jeymi Cano, Universidad de Colombia, proceso de concientización<br>SANS Institute; Computer Security Education and Information | |
| **Xcon6**<br>Frecuencia:<br>6 Meses | Número de empleados que asisten por audiencia en un período de 6 meses.<br>Objetivo.- Determinar el porcentaje total de empleados de determinada área que asisten por audiencia. |
| Fuentes de referencia: Jeymi Cano, Universidad de Colombia, proceso de concientización<br>SANS Institute; Computer Security Education and Information | |
| **Xcon7**<br>Frecuencia:<br>6 Meses | Número total de tópicos que buscan revisarse en las actividades de concientización.<br>Objetivo.- Determinar el número total de tópicos que quieren revisarse en los cursos de capacitación. |
| Fuentes de referencia: Jeymi Cano, Universidad de Colombia, proceso de concientización<br>SANS Institute; Computer Security Education and Information | |
| **Xcon8**<br>Frecuencia:<br>6 Meses | Número de tópicos que realmente se ven en las actividades de concientización.<br>Objetivo: Determinar el número de tópicos que se ven en las actividades de concientización. |
| Fuentes de referencia: Jeymi Cano, Universidad de Colombia, proceso de concientización | |

| | |
|---|---|
| SANS Institute; Computer Security Education and Information | |
| **Xcon9**<br>Frecuencia:<br>6 Meses | Número de actividades de concientización a las que asiste un empleado en un período de 6 meses.<br>Objetivo.- Determinar el número de actividades totales a las que asistió un empleado |
| Fuentes de referencia: Jeymi Cano, Universidad de Colombia, proceso de concientización<br>SANS Institute; Computer Security Education and Information | |
| **Xcon10**<br>Frecuencia:<br>6 Meses | Total de horas que dura un empleado en entrenamiento en un período de 6 meses<br>Objetivo: Tener el número total de horas de entrenamiento que recibe un empleado |
| Fuentes de referencia: Jeymi Cano, Universidad de Colombia, proceso de concientización<br>SANS Institute; Computer Security Education and Information | |
| **Xcon11**<br>Frecuencia:<br>6 Meses | Número total de empleados que asisten a mas horas de entrenamiento en actividades de concientización<br>Objetivo.- Determinar el número de horas promedios a las que asisten los empleados a actividades de concientización |
| Fuentes de referencia: Jeymi Cano, Universidad de Colombia, proceso de concientización<br>SANS Institute; Computer Security Education and Information | |
| **Xcon14**<br>Frecuencia:<br>6 Meses | Número de reportes de incidentes levantados en un período de 6 meses<br>Objetivo: Determina en que porcentaje hay un incremento o disminución de reportes de incidentes de seguridad debido al proceso de concientización |
| Fuentes de referencia: Shannon Anderson, Total information Awareness<br>CERT Coordination center; Computer Emergency Response Team<br>SANS Institute; Computer Security Education and Information | |
| **Xcon15**<br>Frecuencia:<br>6 Meses | Número de personas que han tomado cursos de concientización y que levantaron reporte de incidentes en un período de 6 meses<br>Objetivo.- Expresa el número de personas concientizadas que levantan reportes de inseguridad |
| Fuentes de referencia: Jeymi Cano, Universidad de Colombia, proceso de concientización<br>SANS Institute; Computer Security Education and Information | |

## Proceso política corporativa.

| | |
|---|---|
| **Xpol9**<br>Frecuencia:<br>6 meses | Número de políticas que son actualizadas<br>Objetivo.- Determinar una métrica del % de políticas Actualizadas |
| Fuentes de referencia: Bereau Conseil; Guía para la elaboración de políticas<br>Bereau Conseil; Política de seguridad en sistemas de información.<br>Cicese; Política oficial de seguridad | |
| **Xpol10** | Número de políticas que son auditadas |

| | |
|---|---|
| Frecuencia:<br>1 año | Objetivo.- Determinar una métrica del % de políticas auditadas |
| Fuentes de referencia: Bereau Conseil; Guía para la elaboración de políticas<br>Bereau Conseil; Política de seguridad en sistemas de información.<br>Cicese; Política oficial de seguridad | |

## Proceso Equipo de respuesta a incidentes.

| Variables | Descripción. |
|---|---|
| **Xeri8**<br>Frecuencia:<br>6 meses | Número de incidentes de gravedad media en un período de 6 meses<br>Objetivo.- Con base a estadísticas determinar el número de incidentes de gravedad media, es decir entre graves y de baja gravedad que ocurren en un tiempo determinado |
| Fuentes de referencia: Software Engineering Institute, Computer Incident Response Team<br>NIST (Security self- Assessment guide for information technology systems | |
| **Xeri9**<br>Frecuencia:<br>6 meses | Número de incidentes de baja gravedad en un período de 6 meses<br>Objetivo.- Con base a estadísticas determinar el número de incidentes de baja gravedad ocurren en un tiempo determinado |
| Fuentes de referencia: Software Engineering Institute, Computer Incident Response Team<br>NIST (Security self- Assessment guide for information technology systems | |
| **Xeri10**<br>Frecuencia:<br>6 meses | Número de incidentes resueltos en la primera llamada por help-desk en un período de 6 meses<br>Objetivo.- Determinar el porcentaje de incidentes que se resuelven por help-desk en la primera llamada |
| Fuentes de referencia: Software Engineering Institute, Computer Incident Response Team | |
| **Xeri11**<br>Frecuencia:<br>6 meses | Tiempo de respuesta en el que se resuelve un incidente desde que se detecta hasta que se soluciona<br>Objetivo.- Determina el tiempo promedio en que se resuelve un incidente desde que se detecta hasta que se soluciona |
| Fuentes de referencia: Software Engineering Institute, Computer Incident Response Team | |
| **Xeri12**<br>Frecuencia:<br>6 meses | Número de incidentes de ataques documentados en un período de 6 meses<br>Objetivo.- Determinar el número de ataques que son documentados del total de incidentes ocurridos |
| Fuentes de referencia: Software Engineering Institute, Computer Incident Response Team<br>NIST (Security self- Assessment guide for information technology systems | |
| **Xeri13**<br>Frecuencia:<br>6 meses | Número de incidentes resueltos exitosamente en un período de 6 meses<br>Objetivo.- Determina el número de incidentes que son resueltos exitosamente |
| Fuentes de referencia: Software Engineering Institute, Computer Incident Response Team | |
| **Xeri14** | Número de incidentes que no son resueltos exitosamente en un período de 6 meses |

| | |
|---|---|
| Frecuencia:<br>6 meses | Objetivo.- Determina el número de incidentes que no son resueltos exitosamente |
| Fuentes de referencia: Software Engineering Institute, Computer Incident Response Team | |
| **Xeri21**<br>Frecuencia:<br>6 meses | Número de aplicaciones o programas no autorizados en la empresa en un período de 6 meses<br>Objetivo.- Determina el número de aplicaciones piratas o sin licencia |
| Fuentes de referencia: Software Engineering Institute, Computer Incident Response Team | |
| **Xeri22**<br>Frecuencia:<br>6 meses | Número de actualizaciones al programa ERI en un período de 6 meses<br>Objetivo.- Determina si se realizan actualizaciones al programa constantemente |
| Fuentes de referencia: Software Engineering Institute, Computer Incident Response Team | |

## Proceso análisis de riesgo

| Variables | Descripción. |
|---|---|
| **Xirm4**<br>Frecuencia:<br>1 año | Número de riesgos del total de sistemas, que son aceptados y no se les da seguimiento<br>Objetivo: Determinar el número total de riesgos del total de sistemas que no se les da seguimiento por alguna razón |
| Fuentes de referencia: SANS Institute; Computer Security Education and Information<br>CERT Coordination center; Computer Emergency Response Team<br>NIST National Institute of Standards and technology, Risk Management<br>IRM Information Risk Management; IRM training | |
| **Xirm5**<br>Frecuencia:<br>1 año | Número de riesgos mitigados en un período de 1 año<br>Objetivo.- Determinar el número de riesgos mitigados en un período de 1 año |
| Fuentes de referencia: SANS Institute; Computer Security Education and Information<br>CERT Coordination center; Computer Emergency Response Team<br>NIST National Institute of Standards and technology, Risk Management<br>IRM Information Risk Management; IRM training | |
| **Xirm6**<br>Frecuencia:<br>1 año | Número de vulnerabilidades o debilidades descubiertas en un período de 1 año<br>Objetivo.- Utilizar esta variable para determinar tiempo promedio de respuesta entre que la debilidad es descubierto y la implementación de la acción correctiva<br>datos necesarios # vulnerabilidades que se detectan en 30, 60,90, 180,360 días |
| Fuentes de referencia: SANS Institute; Computer Security Education and Information<br>CERT Coordination center; Computer Emergency Response Team<br>NIST National Institute of Standards and technology, Risk Management<br>IRM Information Risk Management; IRM training | |
| **Xirm7**<br>Frecuencia:<br>1 año | Número de sistemas con IRM que son revisados por dirección general en un período de 1 año<br>Objetivo.- Determinar el grado de involucramiento de la dirección |

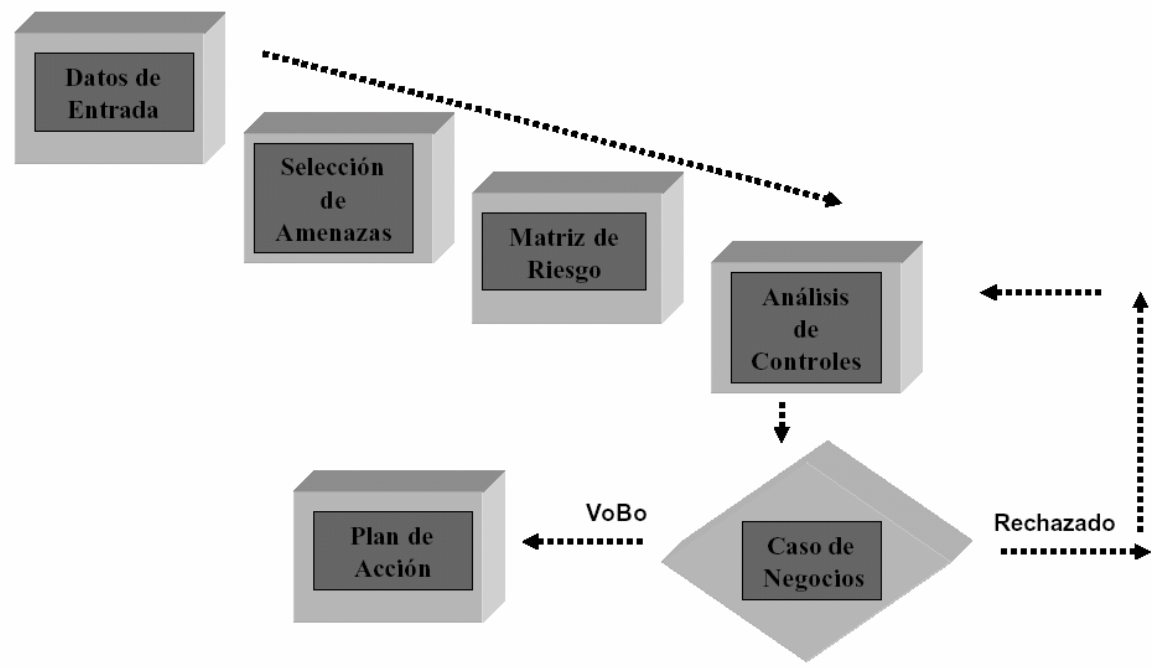
| | |
|---|---|
| Fuentes de referencia: SANS Institute; Computer Security Education and Information<br>CERT Coordination center; Computer Emergency Response Team<br>NIST National Institute of Standards and technology, Risk Management<br>IRM Information Risk Management; IRM training | |
| **Xirm8**<br>Frecuencia:<br>1 año | Número de activos críticos para los cuales el costo por daño perdida ha sido cuantificado en un período de 1 año<br>Objetivo.- Determinar el número de activos totales cuyo costo por daño o perdida ha sido cuantificado |
| Fuentes de referencia: SANS Institute; Computer Security Education and Information<br>CERT Coordination center; Computer Emergency Response Team<br>NIST National Institute of Standards and technology, Risk Management<br>IRM Information Risk Management; IRM training | |

## *Monitoreo de controles de análisis de riesgo.*

Adicionalmente a la aportación de variables construiremos un modelo de monitoreo para controles de análisis de riesgo.

Como se menciono en el proceso de análisis de riesgo las etapas que este proceso comprende son las siguientes.

**Procesos análisis de riesgos**




En la parte de análisis de controles es donde se establecen los controles que ayudarán a mitigar los riesgos. Este análisis determina la cantidad de controles que son necesarios.

En la práctica se ha detectado que existe un conjunto de controles que son comunes a cualquier análisis de riesgos. Es decir, existe un conjunto de controles mínimos necesarios que necesitan estar presentes para mitigar las amenazas en cualquier conjunto de controles derivados del análisis de riesgos.

El conjunto de controles que son comunes se pueden encontrar dentro del contenido del BS7799 como se muestra en la siguiente grafica, a su vez se muestra el control tecnológico.

| Control del BS-7799 | Control Tecnológico |
|---|---|
| 8.3.1 Controls against malicious software<br>6.3.2 Reporting security weaknesses | Enterprise Security Manager de Symantec |
| 8.1.2 Operational Change Control<br>8.3.1 Controls against malicious software<br>6.3.3 Reporting software malfunctions | Tripwire for Servers |
| 9.7.2 Monitoring System Use | SystemEDGE |
| 8.4.1 Information back-up | Networkers |
| 8.3.1 Controls against malicious software<br>6.3.2 Reporting security weaknesses | Nessus |
| 8.3.1 Controls against malicious software<br>6.3.2 Reporting security weaknesses | MBSA |

Tabla 13.- Relación de controles BS-7799 con controles tecnológicos

Los controles tecnológicos se muestran a continuación con más detalle.

- Enterprise Security Manager de Symantec (Software para administración de Vulnerabilidades). Para todo tipo de servidores (Unix, Windows, Linux, etc.)

- Tripwire for Servers (Software para control de cambios en archivos y directorios; te detecta cambios no autorizados). Para todo tipo de servidores (Unix, Windows, Linux, etc.)

- SystemEDGE (Software para monitoreo de desempeño, capacidad y salud del servidor). Para todo tipo de servidores (Unix, Windows, Linux, etc.)

- Networkers (Software para realizar respaldos de los servidores vía remota hacia un sistema de respaldos centralizado). Para todo tipo de servidores (Unix, Windows, Linux, etc.)

- Nessus (Software para detectar vulnerabilidades en servidores: puertos abiertos, parches no instalados, malas configuraciones, etc.). Para todo tipo de servidores (Unix, Windows, Linux, etc.)

- MBSA (Microsoft Baseline Security Analizer) Software para detectar vulnerabilidades en servidores de Windows únicamente: puertos abiertos, parches no instalados, malas configuraciones, etc.)

El objetivo es construir un modelo de variables e indicadores que nos ayuden a monitorear el funcionamiento y efectividad de estos controles así como el estado de los mismos.

El modelo propuesto de monitoreo de controles se define dentro de la etapa de análisis de controles y consiste en agregar el siguiente ciclo.

**Modelo de monitoreo de controles**

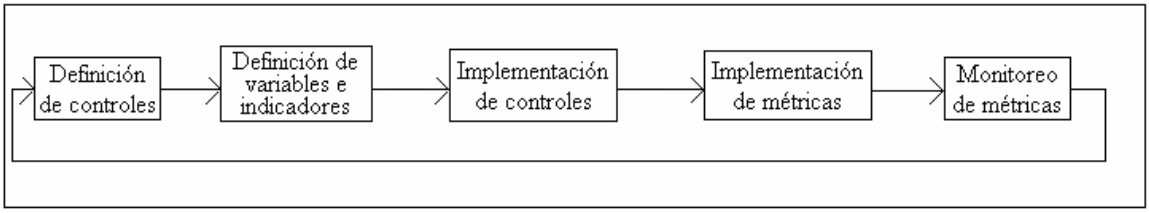



Figura 6.- Modelo de monitoreo de controles.

Las variables que utilizaremos para el monitoreo de estos controles las tomaremos del modelo revisado por la empresa de telecomunicaciones para darle una perspectiva mas practica a este objetivo.

Cabe mencionar que las variables fueron modificadas para monitorear estos controles pero el sentido original de las variables sigue siendo el mismo.

Las variables e indicadores que podemos utilizar se listan a continuación.

Tabla 14.- Variables e indicadores del baseline de controles

**Para el Control de Enterprise Security Manager de Symantec**

| Variables | Descripción. |
|---|---|
| **Xesm1**<br>Frecuencia:<br>6 Meses | Número de reportes de incidentes reportados en un período de 6 meses<br>Objetivo.- Determinar en que porcentaje hay un incremento o disminución de reportes de incidentes de seguridad |
| Con relación a X´con11 | |
| **Xesm2**<br>Frecuencia:<br>6 Meses | Período de tiempo en que se realizan revisiones o auditorias al software para verificar su buen funcionamiento<br>Objetivo.- Establece un período de tiempo para verificar que la configuración del software esta acorde a las necesidades de la empresa para garantizar el buen funcionamiento, en promedio será 6 meses, puede ser mayor o menor tiempo. |
| Con relación a X´con2 | |
| **Xesm3**<br>Frecuencia:<br>6 meses | Número de políticas manejadas por el software<br>Objetivo.- Determinar el número total de políticas manejadas por el software |
| Con relación a X´pol3 | |
| **Xesm4**<br>Frecuencia:<br>6 meses | Número de políticas especificas que han sido violadas<br>Objetivo.- Ayudará a determinar el % de políticas que han sido violadas |
| Con relación a X´pol4 | |
| **Xesm5**<br>Frecuencia: | Número de políticas que son actualizadas<br>Objetivo: Determinar una métrica del % de políticas Actualizadas |

| | |
|---|---|
| 1 año | |
| Con relación a X´pol5 | |
| **Xesm6**<br>Frecuencia:<br>1 año | Número de políticas que son auditadas<br>Objetivo: Determinar una métrica del % de políticas auditadas |
| Con relación a X´pol6 | |
| **Xesm7**<br>Frecuencia:<br>1 año | Número de políticas nuevas creadas<br>Objetivo.- Determinar el número de nuevas políticas creadas en un período de tiempo determinado |
| Con relación a X´pol7 | |
| **Xesm8**<br>Frecuencia:<br>3 meses | Número de vulnerabilidades o debilidades críticas descubiertas por activo.<br>Objetivo.- Conocer el total de vulnerabilidades críticas por activo |
| Con relación a Xirm8 | |
| **Xesm9**<br>Frecuencia:<br>3 meses | Número de vulnerabilidades críticas reparadas vs. no reparadas por activo<br>Objetivo.- Conocer el total de vulnerabilidades críticas vs. no críticas por activo, conocer el tiempo promedio de reparación y de no reparación de vulnerabilidades críticas |
| Con relación a Xirm9 | |
| **Xesm10**<br>Frecuencia:<br>1 año | Número de nuevas vulnerabilidades que se les da seguimiento desde el último reporte<br>Objetivo.- Determinar el número total de vulnerabilidades que se les da seguimiento desde el último reporte |
| Con relación a Xirm13 | |
| **Xesm11**<br>Frecuencia:<br>Mensual | Número total de activos que son actualizados con sus parches de seguridad<br>Objetivo.-Determinar el número total de activos que reciben sus parches de seguridad. |
| Nueva variable | |
| **Xesm12**<br>Frecuencia:<br>Mensual | Número total de activos que son actualizados con sus service pack.<br>Objetivo.-Determinar el número activos que se les instala todos sus service pack. |
| Nueva Variable | |
| **Xesm13**<br>Frecuencia:<br>1 año | Número de incidentes relacionados con código malicioso en un período de 6 meses<br>Objetivo: Determina el número de ataques relacionados con código malicioso(Este pude ser virus, spyware, adware, etc) |
| Con relación a X´eri19 | |
| **Xesm14**<br>Frecuencia:<br>1 año | Número de incidentes relacionados con ataques de Spam en un período de 6 meses<br>Objetivo: Determina el número de ataques relacionados con Spam que ocurren en un tiempo determinado |
| Con relación a X´eri23 | |

Los indicadores son los siguientes.

| Indicadores | Descripción. |
|---|---|
| INDesm1 | Porcentaje de incremento o disminución de reportes de incidentes que se levantaron periódicamente (cada 6 meses) para los activos en monitoreo.<br>Fórmula = Xesm1 – (Número del último reporte de incidentes) |
| INDesm2 | Porcentaje de políticas especificas que han sido violadas por los usuarios<br>Fórmula = Xesm4*100/Xesm3 |
| | |
| INDesm3 | Porcentaje de políticas actualizadas<br>Fórmula = Xesm5*100/Xesm3 |
| | |
| INDesm4 | Porcentaje de políticas que son auditadas<br>Fórmula = Xesm6*100/Xesm3 |
| | |
| INDesm5 | Número de políticas nuevas creadas periódicamente<br>Fórmula = Xesm6 |
| | |
| INDesm6 | Número de vulnerabilidades o debilidades críticas descubiertas por activo.<br>Fórmula = Xesm8 |
| | |
| INDesm7 | Número de nuevas vulnerabilidades descubiertas desde el último reporte<br>Fórmula = Xesm10 |
| | |
| INDesm8 | Porcentaje de activos que son actualizados con sus parches de seguridad<br>Fórmula = Xesm11*100/número total de activos monitoreados por el software |
| | |
| INDesm9 | Porcentaje de activos que son actualizados con sus service pack<br>Fórmula = Xesm12*100/número total de activos monitoreados por el software |
| | |
| INDesm10 | Porcentaje de incidentes relacionados con código malicioso.<br>Fórmula = Xesm13*100/Xesm1 |
| | |
| INDesm11 | Porcentaje de incidentes relacionados con SPAM<br>Fórmula = Xesm14*100/Xesm1 |
| | |

### Para el Control de Tripwire for servers

Las variables e indicadores considerados para este software son:

| Variables | Descripción. |
|---|---|
| **Xtfs1**<br>Frecuencia:<br>6 Meses | Período de tiempo en que se realizan revisiones o auditorias al software para verificar su buen funcionamiento<br>Objetivo.- Establece un período de tiempo para verificar que la configuración del software esta acorde a las necesidades de la empresa para garantizar el buen funcionamiento, en promedio será 6 meses, puede ser mayor o menor tiempo. |
| Con relación a X´con2 | |
| **Xtfs2**<br>Frecuencia:<br>6 meses | Número de incidentes que ocurren en un tiempo determinado.<br>Objetivo.- Determinar el número total de incidentes que ocurren en un tiempo determinado. |
| Con relación a X´pol1 | |
| **Xtfs3**<br>Frecuencia:<br>1 año | Número de logs generados por el software que son respaldadas periódicamente<br>Objetivo.- Construir una métrica que ayude a determinar el porcentaje de logs generados por el software que son respaldados. |
| Nueva variable | |
| **Xtfs4**<br>Frecuencia:<br>1 año | Número de incidentes relacionados con cambios no autorizados en un período de 6 meses<br>Objetivo: Determina el número de accesos no autorizados/ cambios no autorizados que ocurren en un tiempo determinado |
| Con relación a X´eri21 | |
| **Xtfs5**<br>Frecuencia:<br>1 año | Número de incidentes debido a cambios no autorizados documentado(ataque llevados a la etapa de revisión y seguimiento) en un período de 6 meses<br>Objetivo: Determina el número de incidentes que son documentados (llevados a la etapa de revisión y seguimiento) del total de incidentes ocurridos. |
| Con relación a X´eri13 | |
| **Xtfs6**<br>Frecuencia:<br>1 mes | Número de cambios críticos no autorizados detectados por el software<br>Objetivo: Determina el número de cambios críticos detectados por el software |
| Nueva variable | |
| **Xtfs7**<br>Frecuencia:<br>1 mes | Número de cambios críticos no autorizados detectados en archivos<br>Objetivo: Determina el número de cambios críticos sobre archivos |
| Nueva variable | |
| **Xtfs8**<br>Frecuencia:<br>1 mes | Número de cambios críticos no autorizados detectados en directorios<br>Objetivo: Determina el número de cambios críticos sobre directorios |
| Nueva variable | |
| **Xtfs9**<br>Frecuencia: | Número de cambios críticos no autorizados de severidad alta<br>Objetivo: Determina el número de cambios críticos sobre directorios |

| | |
|---|---|
| 1 mes | |
| Nueva variable | |
| **Xtfs10**<br>Frecuencia:<br>1 mes | Número de cambios críticos no autorizados de severidad media<br>Objetivo: Determina el número de cambios críticos sobre directorios |
| Nueva variable | |
| **Xtfs11**<br>Frecuencia:<br>1 mes | Número de cambios críticos no autorizados de severidad baja<br>Objetivo: Determina el número de cambios críticos sobre directorios |
| Nueva variable | |
| **Xtfs12**<br>Frecuencia:<br>1 mes | Diferencia entre los cambios autorizados y los no autorizados<br>Objetivo: Determina la diferencia entre cambios que estaban autorizados y los no autorizados |
| Nueva variable | |

Los indicadores construidos son los siguientes.

| Indicadores | Descripción. |
|---|---|
| INDtfs1 | Período de tiempo en que se realizan revisiones a la configuración del software para garantizar su correcto funcionamiento.<br>Fórmula = Xtfs1 |
| | |
| INDtfs2 | Número de incidentes relacionados a cambios no autorizados en un período de 6 meses<br>Fórmula = Xtfs4*100/Xtfs2 |
| | |
| INDtfs3 | Porcentaje de incidentes relacionados a cambios no autorizados que son documentados<br>Fórmula = Xtfs5*100/Xtfs2 |
| | |
| INDtfs4 | Porcentaje de logs generados por el software que son respaldados<br>Fórmula = Xtfs3*100/ Número total de logs generados por el software |
| | |
| INDtfs5 | Porcentaje de cambios críticos detectados en archivos<br>Fórmula = (Xtfs7*100)/Xtfs6 |
| | |
| INDtfs6 | porcentaje de cambios críticos detectados en directorios<br>Fórmula = Xtfs8*100/Xtfs6 |
| | |
| INDtfs7 | Porcentaje de cambios de severidad alta |

| | |
|---|---|
| | Fórmula = Xtfs9*100/Xtfs6 |
| | |
| INDtfs8 | Porcentaje de cambios de severidad media<br>Fórmula = Xtfs10*100/Xtfs6 |
| | |
| INDtfs9 | Porcentaje de cambios de severidad baja<br>Fórmula = Xtfs11*100/Xtfs16 |
| | |
| INDtfs10 | Diferencia entre los cambios autorizados y los no autorizados<br>Fórmula = Xtfs12 = cambios no autorizados – cambios autorizados |
| | |

## Para el Control del software eHealth systemEdge

Las métricas propuestas son las siguientes.

| Variables | Descripción. |
|---|---|
| **Xhse1**<br>Frecuencia:<br>6 Meses | Número de reportes de incidentes levantados en un período de 6 meses<br>Objetivo.- Determinar en que porcentaje hay un incremento o disminución de reportes de incidentes de seguridad debido al proceso de concientizacion |
| Con relación a X´con11 | |
| **Xhse2**<br>Frecuencia:<br>6 Meses | Período de tiempo en que se realizan revisiones o auditorias al software para verificar su buen funcionamiento<br>Objetivo.- Establece un período de tiempo para verificar que la configuración del software esta acorde a las necesidades de la empresa para garantizar el buen funcionamiento, en promedio será 6 meses, puede ser mayor o menor tiempo. |
| Con relación a X´con2 | |
| **Xhse3**<br>Frecuencia:<br>Mensual | Número total de activos que están siendo monitoreados con el software<br>Objetivo.-Determinar el número de activos de la organización que están siendo monitoreados por el software. |
| Con relación a X´eri1 | |
| **Xhse4**<br>Frecuencia:<br>1 mes | Número de servicios en servidores que son dados de baja<br>Objetivo.- Determinar el número total de servicios que son dados de baja en los servidores |
| Nueva variable | |
| **Xhse5**<br>Frecuencia: | Número de procesos en servidores que son dados de baja<br>Objetivo.- Determinar el número total de procesos que son dados de baja en servidores |

| | |
|---|---|
| 1 mes | |
| Nueva variable | |
| **Xhse6**<br>Frecuencia:<br>1 mes | Número de CPUs que tienen un desempeño optimo (por ejemplo un desempeño del 90 % o superior)<br>Objetivo.- Determinar el número total de CPUs que tienen un desempeño optimo |
| Nueva variable | |
| **Xhse7**<br>Frecuencia:<br>1 mes | Número de tarjetas de red que tienen un desempeño optimo (por ejemplo un desempeño del 90 % o superior)<br>Objetivo.- Determinar el número total de tarjetas de red que tienen un desempeño optimo |
| Nueva variable | |
| **Xhse8**<br>Frecuencia:<br>1 mes | Número de Discos duros que tienen un desempeño optimo (por ejemplo un desempeño del 90 % o superior)<br>Objetivo.- Determinar el número total de discos duros que tienen un desempeño optimo |
| Nueva variable | |
| **Xhse9**<br>Frecuencia:<br>1 mes | Número de memorias que tienen un desempeño optimo (por ejemplo un desempeño del 90 % o superior)<br>Objetivo.- Determinar el número total de memorias que tienen un desempeño optimo |
| Nueva variable | |
| **Xhse10**<br>Frecuencia:<br>1 mes | Número de equipos que están fuera de servicios por fallas<br>Objetivo.- Determinar el número total de equipos que están fuera por fallas |
| Nueva variable | |
| **Xhse11**<br>Frecuencia:<br>1 mes | Número de equipos que están fuera de servicios por mantenimiento<br>Objetivo.- Determinar el número total equipos que están fuera por mantenimiento |
| Nueva variable | |

Los indicadores son los siguientes:

| Indicadores | Descripción. |
|---|---|
| INDhse1<br>Frecuencia:<br>1 mes | Número de reportes de incidentes levantados en un período de 6 meses<br>Fórmula = Xhse1 |
| | |
| INDhse2<br>Frecuencia:<br>1 mes | Período de tiempo en que se realizan revisiones o auditorias al software para verificar su buen funcionamiento<br>Fórmula = Xhse2 |
| | |
| INDhse3<br>Frecuencia:<br>1 mes | Número de servicios en servidores que son dados de baja<br>Fórmula = Xhse16 |

| | |
|---|---|
| Nuevo indicador | |
| INDhse4<br>Frecuencia:<br>1 mes | Número de procesos en servidores que son dados de baja<br>Fórmula = Xhse17 |
| Nuevo indicador | |
| INDhse5<br>Frecuencia:<br>1 mes | Porcentaje de CPUs que tienen un desempeño optimo<br>Fórmula = Xhse6*100/Xhse3 |
| Nuevo indicador | |
| INDhse6<br>Frecuencia:<br>1 mes | Porcentaje de tarjetas de red que tienen un desempeño optimo<br>Fórmula = Xhse7*100/Xhse3 |
| Nuevo indicador | |
| INDhse7<br>Frecuencia:<br>1 mes | Porcentaje de discos duros que tiene un desempeño optimo<br>Fórmula = Xhse8*100/Xhse3 |
| Nuevo indicador | |
| INDhse8<br>Frecuencia:<br>1 mes | Porcentaje de memorias que tienen un desempeño optimo<br>Fórmula = Xhse9*100/Xhse3 |
| Nuevo indicador | |
| INDhse9<br>Frecuencia:<br>1 mes | Porcentaje de equipos que se encuentran fuera de servicio por fallas<br>Fórmula = Xhse10*100/Xhse3 |
| Nuevo indicador | |
| INDhse10<br>Frecuencia:<br>1 mes | Porcentaje de equipos que se encuentran fuera de servicio por mantenimiento<br>Fórmula = Xhse11*100/Xhse3 |
| Nuevo indicador | |

## Para el Control del software Networkers

| Variables | Descripción. |
|---|---|
| Xnet1<br>Frecuencia:<br>6 Meses | Número de reportes de incidentes relacionados a respaldos reportados en un período de 6 meses<br>Objetivo.- Determinar en que porcentaje hay un incremento o disminución de reportes de incidentes de seguridad |
| Con relación a X´con11 | |
| Xnet2<br>Frecuencia:<br>6 Meses | Período de tiempo en que se realizan revisiones o auditorias al software para verificar su buen funcionamiento<br>Objetivo.- Establece un período de tiempo para verificar que la configuración del software esta acorde a las necesidades de la empresa para garantizar el buen funcionamiento, en promedio será 6 meses, puede ser mayor o menor tiempo. |
| Con relación a X´con2 | |
| **Xnet3** | Número de políticas especificas sobre respaldo |

| | |
|---|---|
| Frecuencia:<br>6 meses | Objetivo.- Ayudará a determinar el % de políticas que existen referentes al proceso de respaldo |
| Variable nueva | |
| **Xnet4**<br>Frecuencia:<br>6 meses | Número de políticas referentes al proceso de respaldo que se cumplen correctamente<br>Objetivo: Determinar una métrica del % de políticas que se cumplen correctamente |
| Variable nueva | |
| **Xnet5**<br>Frecuencia:<br>1 mes | Número de respaldos que son generados en total<br>Objetivo.- Determinar el número total de respaldos que se obtienen de los activos |
| Variable nueva | |
| **Xnet6**<br>Frecuencia:<br>1 mes | Número de respaldos que se generan exitosamente(sin errores)<br>Objetivo.- Determinar el número total de respaldos que se obtienen de los activos |
| Variable nueva | |
| **Xnet7**<br>Frecuencia:<br>1 mes | Número de respaldos que son probados para garantizarse como validos<br>Objetivo.- Determinar el número total de respaldos que se obtienen de los activos |
| Variable nueva | |
| **Xnet8**<br>Frecuencia:<br>1 mes | Número de respaldos que tienen errores<br>Objetivo.- Determinar el número total de respaldos que tienen errores |
| Variable nueva | |
| **Xnet9**<br>Frecuencia:<br>1 mes | Número de respaldos que son probados inválidos (que no funcionan correctamente)<br>Objetivo.- Determinar el número total de respaldos inválidos |
| Variable nueva | |
| **Xnet10**<br>Frecuencia:<br>1 mes | Número de servidores no respaldados<br>Objetivo.- Determinar el número total de respaldos que se obtienen de los activos |
| Variable nueva | |

Los indicadores son los siguientes

| Indicadores | Descripción. |
|---|---|
| INDnet1<br>Frecuencia:<br>1 mes | Porcentaje de incremento o disminución de reportes de incidentes relacionados a respaldos que se levantaron periódicamente (cada 6 meses).<br>Fórmula = Xnet1 – (Número del último reporte de incidentes) |
| | |
| INDnet2<br>Frecuencia:<br>1 mes | Porcentaje de políticas de respaldo que se cumplen correctamente<br>Fórmula = Xnet4*100/Xnet3 |
| | |

| | |
|---|---|
| INDnet3<br>Frecuencia:<br>1 mes | Porcentaje de activos con respaldos generados exitosamente<br>Fórmula = Xnet6*100/Xnet5 |
| | |
| INDnet4<br>Frecuencia:<br>1 mes | Porcentaje de respaldos que son probados validos<br>Fórmula = Xnet7*100/Xnet5 |
| | |
| INDnet5<br>Frecuencia:<br>1 mes | Porcentaje de respaldos que tienen errores<br>Fórmula = Xnet8*100/Xnet5 |
| | |
| INDnet6<br>Frecuencia:<br>1 mes | Porcentaje de respaldos que son probados inválidos<br>Fórmula = Xnet9*100/Xnet5 |
| | |
| INDnet7<br>Frecuencia:<br>1 mes | Porcentaje de servidores que no son respaldados<br>Fórmula = Xnet10*100/número total de servidores considerados |
| | |

## Para el Control del software Nessus y MBSA

| Variables | Descripción. |
|---|---|
| **Xnm1**<br>Frecuencia:<br>6 Meses | Número de reportes de incidentes reportados en un período de 6 meses<br>Objetivo.- Determinar en que porcentaje hay un incremento o disminución de reportes de incidentes de seguridad |
| Con relación a X´con11 | |
| **Xnm2**<br>Frecuencia:<br>6 Meses | Período de tiempo en que se realizan revisiones o auditorias al software para verificar su buen funcionamiento<br>Objetivo.- Establece un período de tiempo para verificar que la configuración del software esta acorde a las necesidades de la empresa para garantizar el buen funcionamiento, en promedio será 6 meses, puede ser mayor o menor tiempo. |
| Con relación a X´con2 | |
| **Xnm3**<br>Frecuencia:<br>1 mes | Número de vulnerabilidades o debilidades críticas descubiertas por activo.<br>Objetivo.- Conocer el total de vulnerabilidades críticas por activo |
| Con relación a Xirm8 | |
| **Xnm4**<br>Frecuencia:<br>1 mes | Número de nuevas vulnerabilidades que se les da seguimiento desde el último reporte<br>Objetivo.- Determinar el número total de vulnerabilidades que se les da seguimiento desde el último reporte |
| Con relación a Xirm13 | |
| **Xnm5**<br>Frecuencia: | Número de logs generados por el software que son respaldados<br>Objetivo.- Construir una métrica que ayude a determinar el porcentaje de bitácoras que se |

| | |
|---|---|
| 1 mes | tiene respaldada. |
| Nueva variable | |
| **Xnm6**<br>Frecuencia:<br>1 mes | Número de incidentes documentado(ataque llevados a la etapa de revisión y seguimiento) en un período de 6 meses<br>Objetivo: Determina el número de incidentes que son documentados (llevados a la etapa de revisión y seguimiento) del total de incidentes ocurridos. |
| Con relación a X´eri13 | |
| **Xnm7**<br>Frecuencia:<br>1 mes | Número de vulnerabilidades críticas reparadas vs. no reparadas por activo<br>Objetivo.- Conocer el total de vulnerabilidades críticas vs. no críticas por activo, conocer el tiempo promedio de reparación y de no reparación de vulnerabilidades críticas |
| Con relación a Xirm9 | |
| **Xnm8**<br>Frecuencia:<br>1 mes | Número total de activos que sus vulnerabilidades son monitoreados por el software<br>Objetivo.- Determinar el número total de activos |
| | |
| **Xnm9**<br>Frecuencia:<br>1 mes | Número total de activos con registros de puertos abiertos.<br>Objetivo.- Determinar el número total de activos que son propensos a ataque por tener puertos abiertos. |
| | |
| **Xnm10**<br>Frecuencia:<br>1 mes | Número total de activos con registros de puertos cerrados.<br>Objetivo.- Determinar el número total de activos que son propensos a ataque por tener puertos abiertos. |
| | |
| **Xnm11**<br>Frecuencia:<br>1 mes | Número de vulnerabilidades reparadas<br>Objetivo.- Determinar el número total vulnerabilidades que son reparadas |
| | |

Los indicadores son los siguientes

| Indicadores | Descripción. |
|---|---|
| INDnm1 | Porcentaje de incremento o disminución de reportes de incidentes que se levantaron periódicamente (cada 6 meses) para los activos en monitoreo.<br>Fórmula = Xnm1 – (Número del último reporte de incidentes) |
| | |
| INDnm2 | Número de vulnerabilidades o debilidades críticas descubiertas por activo.<br>Fórmula = Xnm3 |
| | |

| | |
|---|---|
| INDnm3 | Número de nuevas vulnerabilidades que se les da seguimiento desde el último reporte<br>Fórmula = Xesm4 |
| | |
| INDnm4 | Porcentaje de logs generados por el software que son respaldados<br>Fórmula = Xnm5*100/ Número total de logs generados por el software |
| | |
| INDnm5 | Porcentaje de incidentes que son documentados<br>Fórmula = Xnm6*100/Xnm1 |
| | |
| INDnm6<br>Frecuencia:<br>3 meses | Número de vulnerabilidades críticas reparadas vs. no reparadas por activo<br>Fórmula = Xnm7 |
| | |
| INDnm7 | Porcentaje de activos con registro de puertos abiertos.<br>Fórmula = Xnm9*100/Xnm8 |
| | |
| INDnm8 | Porcentaje de activos con puertos cerrados<br>Fórmula = Xnm10*100/Xnm8 |
| | |
| INDnm9 | Porcentaje de vulnerabilidades reparadas<br>Fórmula = Xnm11*100/Xnm4 |
| | |

# Capitulo 7.- Conclusiones.

## *Conclusiones*

### 7.1.- Conclusiones

Durante la investigación de este proyecto fue muy difícil encontrar documentos con métricas elaboradas, solamente se encontraron 4 documentos con algunas de ellas, estos documentos se mencionan como referencias bibliográficas.

Mientras se elaboraba el cuadro de variables se tuvo que recurrir además de los documentos encontrados a un profundo análisis de cada proceso de manera que pudiéramos obtener variables y métricas adicionales.

En cada proceso se trato de de construir un cuadro estructural que contuviera un resumen de varias metodologías existentes de estos procesos que fueron investigadas y analizadas, de tal manera que pudieran contener los aspectos mas relevantes de estas diversas metodologías.

En le caso práctico dentro de la empresa de telecomunicaciones fue muy importante desarrollar primeramente una metodología para implementar el modelo de indicadores, en primer lugar determinar el numero de procesos operativos con los que contaba la empresa, en segundo lugar determinar como estaban llevando acabo sus procesos para determinar que variables podrían ser de interés. Los resultados generales fueron la adopción de muchas variables en su forma original, otras fueron modificadas y adaptadas a sus procesos y algunas otras fueron descartas por no tener un sentido para la empresa.

En la realidad la mayoría de las empresas puede tener una metodología de procesos adaptada a sus necesidades, sin embargo para poder utilizar este conjunto de variables, sus procesos deben estar basados en mejores prácticas y metodologías adecuadas, de tal manera que estas variables puedan ser consideradas y darles un seguimiento.

En la mayoría de los casos será necesario realizar algunas modificaciones a las variables e indicadores de tal manera que puedan ser variables con sentido dentro de la organización donde se estén monitoreando.

## 7.2.- Trabajos futuros.

Ya que no existe información de muchas métricas, el conjunto de variables presentados en este trabajo puede ser ampliado. Este trabajo puede ser tomado como punto de partida para la elaboración de un modelo más robusto.

La ayuda y colaboración de personas profesionales y con muchos años de experiencia y práctica en el área, pueden desarrollar un modelo que contenga variables que con mayor sentido dentro de la práctica, es decir encontrar variables que sean extraídas de la experiencia de la implementación de estos proceso en muchas empresas.

Otro trabajo que se podría realizar es el impacto de la medición y seguimiento de estas variables dentro de los procesos de seguridad, posiblemente al buscar medir estas variables se podría entorpecer los procesos.

También se podría trabajar en la elaboración de un software que recopile información de las variables, posiblemente de los sistemas y aplicaciones para contar con pantallas que muestren información estadística de los indicadores.

## 7.3.- Bibliografía.


Ahmad A Abu-Musa(2004); Auditing E-Business: New Challenges for External Auditors; Journal of American Academy of Business, Cambridge. Hollywood: Mar 2004. Vol. 4, Iss. 1/2; pg. 28; Disponible en http://0-gateway.proquest.com.millenium.itesm.mx:80/openurl?url_ver=Z39. 88-2004&res_dat=xri:pqd&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre =article&rft_dat=xri:pqd:did=000000526439501&svc_dat=xri:pqil:fmt=html&req_dat=xri:pqil:pq_clntid=23693

Alejandro Parra(2004); Charla sobre el tema de seguridad de información; Instituto Tecnológico y de Estudios Superiores de monterrey

ALSI (2004),[En línea]; Academia latinoamericana de seguridad; certificación en seguridad de información; módulos 1,2,3,4; Disponible en: http://www.microsoft.com/latam

Arcert (2004), [En línea]; Equipo de respuesta a incidentes de seguridad; ARcert (Coordinación de emergencias en redes teleinformáticas Argentina); Disponible en: http://www.arcert.gov.ar/webs/csirt_faq.html

Arcert II (2004), [En línea]; Creando un Grupo de Respuesta a Incidentes Proceso para iniciar la implementación ARcert (Coordinación de emergencias en redes teleinformáticas Argentina); Disponible en: http://www.arcert.gov.ar/webs/csirt_creacion.html

Bereau Conseil(2004); [En línea]; Guía para la elaboración de políticas; Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information Sous-direction des opérations; documento disponible en: http://www.ssi.gouv.fr/es/confianza/documents/methods/pssi-section2-methodologie-2004-03-03_es.pdf

BCI (S/F), [En línea]; Desarrollo de respuesta; The business continuity institute; Disponible en: http://www.thebci.org/developingresponse.html

Bruce Schneier(2001),[En línea];Insurance and the computer industry; Association for Computing Machinery. Communications of the ACM. New York: Mar 2001. Vol. 44, Iss. 3; pg. 114, 2 pgs; Disponible en: http://0-gateway.proquest.com.millenium.itesm.mx:80/openurl?url_ver=Z39.88-2004&res_dat=xri:pqd&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&rft_dat=xri:pqd:did=000000069582754&svc_dat=xri:pqil:fmt=html&req_dat=xri:pqil:pq_clntid=23693

Bruce Schneir(2001), [En línea]; Managed Security Monitoring: Network Security for the 21st Century; Counterpain ; Disponible en: http://www.counterpane.com/msm.pdf (2001).

Castillo, Di Mare, Díaz, Díez(1004),[En línea]; Concientizacion en la seguridad de la información, Universidad de los Andes, Colombia; Disponible en: http://www.criptored.upm.es/guiateoria/gt_m142r.htm

CICESE (2001), [En línea]; Política oficial de seguridad del CISECE; CICESE; Disponible en: http://telematica.cicese.mx/seguridad/poli-segu.pdf

Chavez (2004); [en línea]; Política de seguridad; seguridad informática; Universidad de los andes, Merida Venezuela; disponible en: http://www.walc2004.cepes.org.pe/apc-aa/archivos-aa/1e60354f4717edb9fb793dbc5219499d/politica2004.pdf

Computerworld (2004), [En línea]; Política de Seguridad Corporativa. Disponible en: http://www.sia.es/sia.es/siapage.asp?id=np270404&b=08s=51,27 de abril 2004

Corporate information security working group "Report of the best practices and metrics teams"(2005);[En línea]; Disponible en: http://www.educause.edu/LibraryDetailPage/666&ID=CSD3661

Doddrell, Gregory R(1995); [En línea]; Security environment reviews ; Information Management & Computer Security. Bradford: 1995. Vol. 3, Iss. 4; pg. 3; Disponible en:http://0-gateway.proquest.com.millenium.itesm.mx:80/openurl?url_ver=Z39.88-2004&res_dat=xri:pqd&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&rft_dat=xri:pqd:did=000000115723748&svc_dat=xri:pqil:fmt=text&req_dat=xri:pqil:pq_clntid=23693

Donald R. Glass(Sin fecha),[on line]; Certified Information Systems Security Professional; Disponible en: URL:http://www.cccure.org/Documents/DonaldGlass/2.AccesControlSystems.pdf

Donald R. Glass(No date),[On line]
TITULO Y SUBTITULO: Certified Information Systems Security Professional
http://www.cccure.org/Documents/DonaldGlass/2_AccessControlSystems.pdf

Donald R. Glass(no fecha)Argentina,[on line]
TITULO Y SUBTITULO: BCP: Business Continuity Plan.
URL:http://www.cccure.org/Documents/DonaldGlass/9-businessContinuityandDisasterRecoveryPlanning.pdf

Dürsteler Juan C.(2003)[En línea]; BAM Visualizando la actividad del negocio; Baquia knoledge center; Disponible en: http://www.baquia.com /noticias. php ?id = 8977.

Espiñeira, Sheldom y Asociados(2003)[En línea];Seguridad de Activos de Información (Parte I y II);Pc-News; Disponible en :http://www.pc-news.com/ detalle.asp?sid=&id=11&Ida=1072, Marzo del 2003

European software institute (2005);[En línea] "Seguridad TIC, Que hay que medir disponible en: http://www.esi.es

Georgia Killcrece(2004),[En línea] pasos basicos para la creación de un CSIRT nacional: Descripción de alto nivel, Carnegie Mellon; Disponible en: www.cicte.oas.org/Docs/ CyberSecurityConference/ES_NationalCSIRTs.doc

Jeimy Cano(2004), [En línea] Concientización en seguridad de la información; Universidad de Bogotá Colombia; disponible en: http://www.criptored.upm.es/guiateoria/gt_m142r.htm

John Markoff, John Schwartz(2003),[En línea]; Sistema de vigilancia del Pentágono(Total Awarennes); Disponible en:
URL: http://www.derechos.org/nizkor/excep/tiaesp.html

Kayzen (2004),[En línea]; Como definir indicadores; Grupo Kayzen; Disponible en: http://www.gestiopolis.com/canales5/ger/gksa/90.htm.

IBM (S/F), [En línea]; Servicios para la continuidad del negocio; monografía patrocinada por IBM; Disponible en: http://www.espaciopyme.com/monograficos/Continuidad_y_recuperacion.pdf

Internet Solution (2005), [En línea]; Seguridad lógica; Internet Solutions; Disponible en: http://www.internet-solutions.com.co/ser_fisica_logica.php

Linda McCarthy(2004), [En línea]; Soporte ejecutivo y Seguridad de TI; Disponible en: http://www.symantec.com/region/mx/enterprisesecurity/ content/expert/ LAM_3320.html; 12 de Marzo de 2004

Mandujano Manuel (2005), [En línea]; Continuidad viva del negocio; Infochanel portal lider del canal de distribución de TI; Disponible en: http://www.infochannel.com.mx/reporte6.asp?id_nota=11186

Martin Botha, Rossouw von Solms(2002),[En línea]; The utilization of trend analysis in the effective monitoring of information security. Part 2: The model;

Information Management & Computer Security. Bradford:
2002. Vol. 10, Iss. 1; pg. 5, 7 pgs; Disponible en:
http://0-gateway.proquest.com.millenium.itesm.mx:80/openurl?url_ver=Z39.88-2004&res_dat=xri:pqd&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&rft_dat=xri:pqd:did=000000208759591&svc_dat=xri:pqil:fmt=html&req_dat=xri:pqil:pq_clntid=23693

M. Farias- Elinos (2003)[En línea]; Auditoría de los Sistemas de Seguridad de la Información; Disponible en: http://seguridad.internet2.ulsa.mx /congresos /2003/univa/ audit_seguridad. pdf

NETSEC(2005);[En línea] "Using metrics to improve security" Disponible en: http://www1.netsec.net/content/securitybrief/archive/2004-09_Metrics.pd

NIST (2005), [En línea]; NIST (Security self- Assessment guide for information technology systems); National Institute of Standards and Technology; Disponible en: http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf

Polytechnic University(2005);[en línea] "Security metrics"; Disponible en: http://isis.poly.edu/courses/cs996-management-s2005/Lectures/SecurityMetrics.ppt

Revista Gerencia(2004), [En línea]; CRM, Seguridad, Procesos administrativos; Revista gerencia; Disponible en:http://www.gerencia.cl/seccion.mv?ids=11

Robert Durst, Terence Champion, Brian Witten, Eric Miller, Luigi Spagnuolo(1999),[En línea]; Testing and evaluating computer intrusion detection systems; Association for Computing Machinery. Communications of the ACM. New York: Jul 1999. Vol. 42, Iss. 7; pg. 53, 9 pgs; Disponible en:
http://0-gateway.proquest.com.millenium.itesm.mx:80/openurl?url_ver=Z39.88-2004&res_dat=xri:pqd&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&rft_dat=xri:pqd:did=000000042834558&svc_dat=xri:pqil:fmt=html&req_dat=xri:pqil:pq_clntid=23693

Robin L Dillon, M Elisabeth Pate-Cornell, Seth D Guikema(2003),[En línea]; Programmatic risk analysis for critical engineering systems under tight resource constraints: Operations Research. Linthicum: May/Jun
2003. Vol. 51, Iss. 3; pg. 354 ; Disponible en:
http://0-gateway.proquest.com.millenium.itesm.mx:80/openurl?url_ver=Z39.88-2004&res_dat=xri:pqd&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&rft_dat=xri:pqd:did=000000354051851&svc_dat=xri:pqil:fmt=html&req_dat=xri:pqil:pq_clntid=23693

Rodríguez Luis (2006), [En línea]; Control de accesos: de la era del mainframe a los PKI; departamento de tratamiento de la información y codificación; Disponible en: http://www.iec.csic.es/criptonomicon/articulos/expertos69.html

Sanderson, Ethan(1996)[En línea];Information Management & Computer Security. Bradford: 1996. Vol. 4, Iss. 1; pg. 32;Information security in business environments; disponible en: http://0-gateway.proquest.com.millenium.itesm.mx:80/openurl?url_ver=Z39.88-004&res_dat=xri:pqd&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&rft_dat=xri:pqd:did=000000115723777&svc_dat=xri:pqil:fmt=text&req_dat=xri:pqil:pq_clntid=23693

Shannon Anderson (S/F), [En línea]; Total information awareness; The Dangers of Using Data Mining Technology to Prevent Terrorism; Defense Comitee; disponible en: http://www.bordc.org/threats/data-mining.pdf

Someswar Kesh, Sam Ramanujan(2004)[En línea]; Model for Web Server Security; Journal of American Academy of Business, Cambridge. Hollywood: Mar 2004. Vol. 4, Iss. 1/2; pg. 354; Disponible en: http://0-gateway.proquest.com.millenium.itesm.mx:80/openurl?url_ver=Z39.88-2004&res_dat=xri:pqd&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&rft_dat=xri:pqd:did=000000526439341&svc_dat=xri:pqil:fmt=html&req_dat=xri:pqil:pq_clntid=23693

Symantec (2004), [En línea]; Artículos de los expertos en seguridad de symantec; Symantec; Disponible en Symantec: http://www.symantec.com/region/mx/enterprisesecurity/content/expert/LAM_1155.html

SVIS-E business(sin fecha),[En línea];Tecnología de Información en su Negocio; Disponible en:URL: http://www.svis.com.mx/presentaciones /archivos/SVIS_Estrategia_de_Seguridad_P-P-008-051103_V1.1.ppt

Universidad Nacional de Colombia (2003), [En línea]; guía para elaboración de políticas de seguridad; Universidad nacional de Colombia; Disponible en: http://www.unal.edu.co/seguridad/documents/guia_para_elaborar_politicas_v1_0.pdf

Victor Cappucio (2002), [En línea]; Políticas y procedimientos en la seguridad de información; ilustrados; Disponible en: http://www.ilustrados.com/publicaciones/EplpVpluZApDVycVbU.php

Villalón Huerta Antonio (2002),[En línea]; Servicios Editoriales para la documentacion libre; Analisis de riesgos; Disponible en: http:// es.tldp.org/ Manuales-LuCAS/doc-unixsec/unixsec-html/node334.html(2002)

Villalón Huerta Antonio (2002),[En línea]; Servicios Editoriales para la documentacion libre; Analisis de riesgos; Disponible en: http:// es.tldp.org/ Manuales-LuCAS/doc-unixsec/unixsec-html/node333.html(2002)