ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“PLAN DE CONTINGENCIA ANTE CIBERATAQUES”

TRABAJO DE TITULACIÓN

Previo a la obtención del título de:

MAGISTER EN TELECOMUNICACIONES

FRANKLIN FARIED FREIRE FAJARDO

GUAYAQUIL – ECUADOR

AÑO: 2017

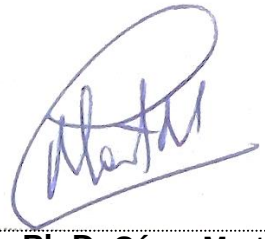
AGRADECIMIENTOS

Agradezco a mis padres, Angela y Flavio, sin su guía y apoyo no hubiera llegado tan alto.

DEDICATORIA

Dedicado a mi esposa Jennifer y mis hijos Amelia y Farid, son mi motivo de superarme cada día.

TRIBUNAL DE EVALUACIÓN



Ph.D. César Martin

SUBDECANO DE LA FIEC

M.Sc. Vladimir Sánchez

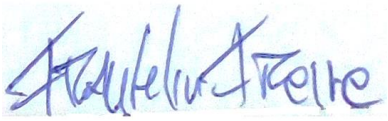
DIRECTOR DEL TRABAJO DE TITULACIÓN

MSIG Albert Espinal

MIEMBRO PRINCIPAL DEL TRIBUNAL

DECLARACION EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, me corresponde exclusivamente; y doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"



Franklin Freire

RESUMEN

Los planes de contingencia cuando se administran centros de cómputo son necesarios para la continuidad del negocio, ya que no solo son datos los que se almacenan y procesan para ofrecer plataformas de noticias, entretenimiento, financieros, entre otros; también es dinero invertido por organizaciones, compras y ventas de clientes, por ende, el tener respaldo informático ante eventos no deseados, como terremotos u otro desastre natural, daños físicos o lógicos de equipos es importante. El presente documento se enfoca en ciberataques, que son daños en la disponibilidad del servicio y desde hace aproximadamente 10 años se han convertido en un problema de seria consideración debido a la pérdida económica que infringen en las organizaciones.

Se propone un plan de contingencia hacia dos direcciones: un centro de cómputo propio en un sitio remoto con una réplica de equipos; y como alternativa, aplicar una contingencia en un Centro de Datos Virtual, que es replicar la información hacia un centro de cómputo con certificación TIER IV.

Las planificaciones para realizar el plan de contingencia deben seguir ciertas normativas y en el presente documento son basadas en el COBIT, aunque también tienen ciertos alcances del ISO 22301 del 2012, que trata de los requisitos necesarios para un sistema de continuidad del negocio.

La propuesta “Plan de Contingencia ante Ciberataques” puede entenderse como un tema netamente técnico, pero en realidad forma parte de un tema amplio como lo son los planes de contingencia, los cuales deben tratarse como proyectos a largo plazo, con una ejecución y mejora continua, ya que se debe dominar las tareas necesarias para pasar de producción a contingencia y luego reversar los cambios en caso de presentarse una emergencia o evento no esperado.

ÍNDICE GENERAL

CAPÍTULO 1

1. Antecedentes

En la actualidad los sistemas informáticos se utilizan en nuestro diario vivir, sea en lo laboral, académico, entretenimiento, información local y del mundo, entre otras. Es tanta la dependencia de esta “siempre en línea” para resolver un problema, mantenerse informado (siendo mucha información falsa (fake) o broma (prank)), Esto nos hace vulnerables a los conocidos “ataques”, ya sean estos con el objetivo de robar información sensible, paralización de sistemas, envío de información falsa o alarmante. Por lo tanto, se ha vuelto una necesidad contar con un plan de emergencia ante estos ataques, ya que no solo pueden inhibir equipos sino también pueden afectar la credibilidad de la empresa y este punto es muy importante hacia los inversionistas y público en general, dado que representa inversión monetaria.

1.1 Descripción del problema

Diversos sistemas actualmente se encuentran interconectados electrónicamente ofreciendo acceso a la información de alta disponibilidad, ya sean estas, noticias o entretenimiento streaming (webex, goto meeting, skype), bibliotecas digitales. La cantidad de usuarios conectándose simultáneamente da para pensar qué sucedería después de un eventual desastre, por ejemplo, un potencial ciberataque.

El ciberataque es una acción llevada por una o más personas con el objetivo de vulnerar falencias conocidas para forzar el acceso a zonas restringidas, por ejemplo: Espacios de archivos de servidores, deshabilitación de seguridad en firewalls, toma de control de computadoras personales, robo de información de bases de datos, cambios de contraseñas, entre otros.

Los ciberataques no solo provocan una indisponibilidad del servicio, sino también pérdidas económicas, esto debido a que los equipos en su mayoría quedan inservibles y las transacciones electrónicas que se procesan diariamente se pierden o quedan en standby para reproceso tardío, lo cual genera trabajo

extra para el personal de la institución y molestias a clientes y ciudadanía en general.

1.2 Justificación

Los planes de contingencia son necesarios para la continuidad del negocio, es decir, las instituciones deben seguir operando con un tiempo mínimo de indisponibilidad y asumir un margen de pérdida económica en el presupuesto anual.

Los planes de contingencia abarcan lo siguiente:

- Duplicidad de enlaces de datos (tener un enlace principal y uno de respaldo) de diferentes proveedores.
- Equipos de red de frontera para realizar conmutación entre la red principal y respaldo, es decir, la institución tendría dos enlaces, uno del centro de cómputo principal y el otro enlace hacia el su centro de cómputo de respaldo, el cual contiene los equipos físicos o virtualizados de los servicios prioritarios.
- Accesos VPN actualizados, licenciados u Open Source.
- Servidores críticos virtualizados en áreas fuera de la institución.
- Los equipos de correo electrónico, homepage, Directorios Activos, DNS y equipos de menor impacto pueden ser puestos en línea al final.
- Las bases de datos, deben estar en equipos principal y respaldo en replica constante.

El plan que se elabore tendrá presente los parámetros antes mencionados para que los servicios suban desde los críticos hasta los de menor importancia; y se debe definir el área a desarrollar el plan, en este caso, se toma el área de sistemas ante un ciberataque.

La planificación, es la sección en donde se elabora la estructura, los pasos a seguir para la recuperación. Dependiendo del tamaño de la organización, se establece un equipo que se encargue del proyecto donde se evaluarán los detalles en un proceso de mejora continua.

La realización del plan de contingencia es la aplicación del proyecto, donde se ejecutará y evaluará el plan establecido durante la planificación, priorizando servicios, análisis y evaluación del proceso de recuperación y sus respectivas pruebas.

El plan de contingencia, como en cualquier proyecto, debe tener un cierre, donde luego de las pruebas y la elección de la estrategia de recuperación se deja la documentación y socialización entre personal técnico relevante que quedara a cargo de la aplicación del plan de continuidad del negocio. Sin embargo, como la tecnología evoluciona constantemente y se debe cambiar equipos, redes y demás procesos que intervienen en el servicio, los planes de contingencia deben estar en un proceso de mejora continua, revisión y ejecución de pruebas al menos 2 veces al año.

1.3 Solución Propuesta

La solución al problema del ciberataque, una vez que los protocolos de identificación y mitigación han fallado, es levantar un sitio alterno, al menos con lo necesario para regresar el sistema al estado “en línea”, tomando en cuenta presupuesto y tipo de contingencia a realizar, ya que existen diferentes tipos de planes de contingencia y a pesar de que todos tienen el mismo fin (salvaguardar el negocio), sus procesos son diferentes y sus grados de requisitos van desde lo básico hasta lo avanzado en lo relacionado a equipamiento y personal.

La realización de la solución puede lograrse con el cumplimiento de los siguientes objetivos:

- Establecer la importancia de la ciberseguridad en empresas privadas o públicas.
- Definir los equipos críticos procese datos de clientes y proveedores.
- Analizar la prioridad de los servicios brindados por la empresa hacia sus clientes.
- Planificar una estrategia de continuidad del negocio.
- Realizar detalladamente la estrategia de continuidad del negocio.

1.4 Metodología

La metodología para la realización de la solución propuesta (levantamiento de sitio alterno) se logra si se cumplen los objetivos de la siguiente manera:

El primer objetivo se conseguirá mediante la revisión bibliográfica acerca de las amenazas más comunes y los eventos más relevantes ocurridos en los últimos 5 años.

El segundo y tercer objetivo, se obtiene mediante la revisión de un centro de cómputo general, el cual contiene los equipos necesarios para los diferentes servicios ofrecidos. Dentro de este grupo, al margen de su importancia, se debe establecer la prioridad del servicio ofrecido por cada equipo.

El cuarto y quinto objetivo, se alcanzarán estableciendo una estrategia de duplicidad o compra de equipos, enlaces de datos o alquiler de alojamiento en la nube.

1.5 Alcance

El plan de contingencia propuesto contará con un análisis técnico y financiero para el establecimiento del costo/beneficio para la empresa, sin que esto represente reducción de plataformas tecnológicas en su calidad o establecimiento de protocolos de contingencia “a medias”.

CAPÍTULO 2

2. ASPECTOS BÁSICOS DE CIBERSEGURIDAD

La ciberseguridad es un aspecto que ha ganado su lugar en el mundo de los negocios, tanto, que las compañías invierten miles de dólares en proteger su infraestructura; en el presente capítulo se expondrán desde el concepto de ciberseguridad hasta los equipos que se encargan de brindar protección en la red.

2.1 CONCEPTO DE CIBERSEGURIDAD

La ciberseguridad se define como “la preservación de confidencialidad, integridad y disponibilidad de la información” [1], pero bajo este concepto también se define la “Seguridad de la información”, con lo que aparece la interrogante: ¿cómo pueden estar correlacionados ambos conceptos entre sí?, a simple vista hacen mención a parámetros diferentes, ya que la ciberseguridad se centra en el ambiente virtual y la seguridad de la información se aplica a las formas tradicionales de gestionar información. Según indica el libro de Dejan Kosutic: “Ciberseguridad en 9 pasos”, la ciberseguridad debe estar libre de peligros y daños ocasionados por interrupciones, caídas de los servicios o abusos de las TIC. El peligro o daño debido al abuso, interrupción o caída de los servicios puede estar constituido por una limitación de la disponibilidad y confiabilidad de las TIC, una violación de la confidencialidad de la información almacenada en las TIC o un daño a la integridad de esa información [2]. Sin embargo, ambos términos pueden intercambiarse indistintamente, ya que ambos representan en última instancia la protección de los datos de usuarios generales, corporaciones o gobiernos. Se puede concluir que la ciberseguridad es la seguridad de la información digital.

2.2 NIVELES DE SEGURIDAD EN LA RED

Las redes de datos han tenido una evolución vertiginosa desde la década de 1960, pasando de conexiones complicadas, poco fiables y costosas a redes sencillas, confiables y bajo costo. De entre las tecnologías que aparecieron y sus protocolos, se pueden mencionar el protocolo IP y las redes LAN (Local Area

Network), y sus versiones MAN (Metropolitan Area Network) y WAN (Wide Area Network).

Los cambios también han llevado a la sociedad de tener archivos físicos (facturas, memorandos, periódicos, etc.), sintonización tradicional de noticias (radio y TV), entretenimiento (programas de concurso, comedias), desplazamiento de un punto a otro hacia la digitalización de estos ejemplos mencionados, como ejemplo, se tiene el envío de las facturas y demás documentos importantes al correo electrónico o vía validación de cuenta (amazon, comisariatos, etc), sintonizar programas radiales y de televisión online (radio online, noticieros online, etc) y tal vez la más relevante ejemplificada en la forma de trabajar actualmente, ya que la mayor parte de las empresas, medianas y pequeñas, que generalmente ofrecen servicios (tecnológicos, ventas, soporte, etc.) ya no necesitan desplazar a su personal hacia el cliente y viceversa, porque los casos de poco y mediano impacto se pueden resolver con herramientas remotas que utilizan la Internet para su gestión y solución.

Sin embargo, con la migración de las personas hacia actividades que empleen recursos tecnológicos, han surgido a su vez problemas en la seguridad, algunos más graves que otros, pero que en algún momento han comprometido los sistemas (lo cual se tratará más a fondo en el capítulo 3).

Los problemas de seguridad que han sufrido los sistemas han dado como resultado la implementación de niveles de seguridad en la red, para no solo aislar un problema y establecer su solución, sino para cotejar grados de responsabilidad (ya sea el usuario o administrador, no descartando que pueda haber falla en el equipo) y establecer protocolos de seguridad.

Los niveles de seguridad en la red pueden clasificarse como:

- Bajo
- Medio
- Alto

El nivel de seguridad bajo se encuentra directamente ligado a los usuarios, porque son el eslabón más débil en toda la red, debido a que, ya sea por un

error involuntario o por malos hábitos de cuidado de la información tanto personal como de acceso a la red corporativa, pueden comprometer equipos como los de producción con un simple acto de leer algún archivo adjunto de correo desconocidos o ingresar a páginas electrónicas que no emplean seguridades. Para evitar en lo posible las consecuencias de estos actos, es necesario establecer autenticación mediante usuario y contraseña, para permitir el ingreso al sistema o aplicación que se necesite. Este nivel es considerado la primera línea de defensa contra los ataques.

El nivel de seguridad medio recae directamente en el cableado estructurado y permisos de acceso; lo que se refiere a seguridad en el cableado, es su acceso, ya que este puede ser intervenido para robar información (conocido como “pinchar”) y esto se relaciona con el lugar de instalación, deber ser inaccesible para personal no autorizado, como techos, paredes, tumbados y pisos falsos. Actualmente en edificios, se habilitan espacios para permitir el paso de cables y solo la administración del edificio se encarga de permitir acceso para instalaciones nuevas y mantenimiento de las existentes.

Los permisos de acceso son los privilegios asignados a un usuario de la red para ingresar al sistema, dependiendo del rol que se asigne a cada usuario, estos tendrán acceso a diferentes recursos de la red compartida localmente o hacia el exterior (internet). Los usuarios con mayor privilegio asignado con generalmente los administradores de sistemas y soporte técnico (con sus respectivas restricciones en producción).

El nivel de seguridad alto está directamente relacionado con los administradores del sistema (servidores, programas, directorios activos, red) y los equipos orientados a la seguridad en la red, tales como firewalls, antivirus y demás. Los administradores y equipos son la última línea de defensa ante un ataque, ya que ellos son los encargados de colocar los filtros y barreras necesarias para custodiar la información transmitida, procesada y almacenada en los servidores y storage, yendo un paso más allá, son los responsables de garantizar la operación con pérdidas mínimas en caso de desastre.

2.3 EQUIPOS ORIENTADOS A SEGURIDAD DE REDES LAN/WAN

Los equipos orientados a la seguridad de redes sean LAN o WAN, son obligatorios en un ambiente empresarial o gubernamental, ya que la información que manejan puede estar siendo “vista” por la competencia o curiosos que desean crear competencia basada en el espionaje.

Los equipos de seguridad solo tienen una función general: evitar acceso no autorizado; bajo esta premisa, los primeros equipos “watch dog” eran muy básicos en cuanto reglas, ya que la filtración se realizaba mediante hardware y trabajaban con direcciones IP o MAC. Luego llegaron los firewall, que no solo realizaban bloqueos de IP y MAC, sino también bloqueo de contenido con respecto al tipo de tráfico entrante y saliente. Estos últimos no dependían del hardware para su procesamiento, sino que las reglas, configuraciones y administración se basaba en software (muchas veces propietario como cisco o checkpoint), lo que lo hacía mucho más versátil al momento de actualizar y de incluir funcionalidades en versiones superiores.

Los equipos orientados a la seguridad de redes se muestran en la figura 2.1:

- Firewalls
- IPS
- WAF
- VPN

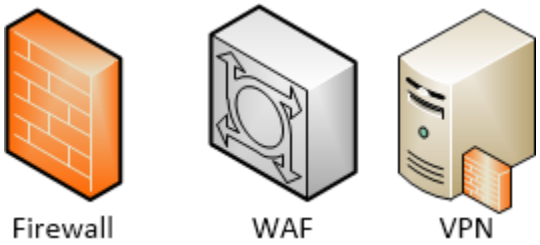


Figura 2.1 Equipos orientados a seguridad de redes

A continuación, una breve descripción de los equipos antes mencionados:

Firewalls: los firewalls o cortafuegos son equipos diseñados para controlar el tráfico que circula en la red interna y externa mediante reglas que, dependiendo

de las políticas de seguridad, podrán ser configuradas en áreas llamadas DMZ. Los firewalls son dispositivos robustos, pero no infalibles ante un posible ciberataque.

Intrusion Prevention System (IPS): los IPS son el sistema de prevención de intrusos cuya función principal es la de monitorear el tráfico de la red, detectar actividad anómala, de acuerdo a las políticas de seguridad implementadas e intentar detenerlas. Actualmente, estos equipos son muy importantes en las redes corporativas y gubernamentales, ya que se puede detectar y detener un ciberataque, sin mencionar la localización del origen de la amenaza.

Web Aplication Firewall (WAF): Se conocen como equipos Web Aplication Firewall (WAF) a firewalls cuya función principal es resguardar las aplicaciones web ante ataques habituales presentes en la red, como ataques DDoS. Puede actuar también como balanceador de carga en el sistema.

Virtual Private Network (VPN): Se entiende como VPN, la conexión de forma segura entre dos redes a través del Internet sin el riesgo de comprometer la información de credenciales o de otra índole. Actualmente es ampliamente utilizada para trabajos remotos o la conexión de distintas áreas a través de Internet, ahorrando costos de enlaces privados. Existen dos clases de implementaciones de VPN, de hardware y de software. Las VPN de Hardware tienen un rendimiento superior y no dependen de otros dispositivos informáticos, como Cisco, Fortinet, etc. Y las de Software, las cuales están limitadas, en su rendimiento por el sistema operativo donde se encuentra instalada la solución (Open VPN, Open SSH, etc).

CAPÍTULO 3

3. CIBERATAQUES REGISTRADOS Y SU IMPACTO

En el presente capítulo se expondrá los ciberataques registrados más importantes alrededor del mundo y sus consecuencias, así como, la definición de un ciberataque, su similitud y diferencia con el Hacking Ético y el impacto cultural que ha tenido durante los últimos 20 años.

3.1 DEFINICIÓN DE CIBERATAQUE

El ciberataque es el acto de infiltrarse de manera ilegal a redes privadas o públicas gubernamentales (no confundir con redes de acceso público), para robar información, generar fallos en la red o servidores implantando virus informáticos y dependiendo de la finalidad del ataque, puede considerarse como ciberdelincuencia, cibercrimen o ciberguerra (conocida también como ciberterrorismo). [2]

Para catalogar o clasificar un ciberataque, es necesario establecer la meta, por ejemplo, la ciberdelincuencia, que encierra todo lo que se refiere a los daños realizados a las computadoras, redes y cualquier equipo informático, utilizando medios tecnológicos. El cibercrimen, en cambio, es realizar un acceso ilegal para robar información, cometer fraude mediante la suplantación de identidad de medios de pago electrónico (comúnmente de tarjetas de crédito), con la finalidad de obtener dinero en su lugar. El ciberterrorismo, es un escalón más arriba, ya que, mediante una serie de técnicas informáticas, se realizan actos contra la población o un grupo de personas para causar daños con fines políticos o ideológicos.

Las clasificaciones de los ciberataques no son realizadas por personas aisladas, al menos en nuestros días ya no. Existen grupos y empresas que se encargan de alquilar sus servicios “al mejor postor”, al estilo de mercenarios. Los gobiernos también contratan y entrenan a ingenieros para contar entre sus filas una defensa contra los ciberataques que pudieran recibir su infraestructura y también para realizar una ofensiva en caso de una ciberguerra.

Los ataques o técnicas de ataque más comúnmente ejecutadas son:

Virus Informático: programas que se encargan de dañar, borrar, reemplazar o capturar ciertos archivos sensibles del sistema operativo, archivos con extensiones predefinidas e instalar archivos que contienen código malicioso y de acuerdo a su programación pueden cometer ciberdelincuencia o cibercrimen.

SPAM: se denomina SPAM al envío masivo de correos electrónicos, generalmente de un remitente desconocido con publicidad, pero que de alguna manera perjudican al receptor o receptores ya que, si son de un mismo dominio, pueden llegar a saturar el servidor de correos provocando una baja de un servicio de comunicación.

BOTS: es una contracción de ROBOT. Se refiere a computadoras que son controladas remotamente para ejecutar una acción determinada, sin conocimiento del usuario real. Los robots, también llamados “zombies”, son muy útiles al momento de un ataque masivo desde diferentes áreas.

3.2 DIFERENCIA ENTRE CIBERATAQUE Y HACKING ÉTICO

La diferencia entre el ciberataque y el hacking ético en esencia es la intención del ejecutante o el grupo que se encarga de ejecutar ciertas tareas. Las herramientas y conocimientos son iguales, pero el ciberataque se aprovecha de las vulnerabilidades en un determinado sistema para realizar un daño o lucrarse de manera ilegal; mientras que el hacking ético encuentra las mismas vulnerabilidades pero también realiza los pasos necesarios para corregir los fallos encontrados y aunque también se facturan por los servicios prestados, no compromete la seguridad corporativa, gubernamental, o información sensible que exista mediante contratos y acuerdos de confidencialidad.

La técnica para encontrar las vulnerabilidades en los sistemas se llama “Pentesting”. Existen distribuciones Linux especializadas y la más popular es Kali Linux. La distribución Kali Linux es utilizada tanto para un cibercrimen como para un hacking ético, por este motivo, el personal de seguridad informática debe realizar pruebas periódicas de pentesting, actualizarse continuamente en nuevas versiones de malware, ataques (internacionales o locales) detectados y

actualizar el sistema (equipos, sistemas operativos y programas asociados) para garantizar la ciberseguridad.

El pentesting, es utilizado ampliamente por los auditores de seguridad informática para la detección de vulnerabilidades en sistemas a nivel lógico. Generalmente son distribuciones Linux que pueden ser instaladas en máquinas virtuales o utilizarse de manera “live” en un CD o Memoria Flash (pendrive); también se utilizan para determinar el éxito o fracaso de un ataque particular y para verificar la defensa del sistema ante un ataque.

El uso del pentesting y sus sistemas operativos especializados fueron concebidos como una herramienta de evaluación de seguridad, por esta razón estos sistemas no deben utilizarse para tareas de usuario en empresas u hogar. Existen técnicas automatizadas incluidas en estos sistemas especializados como el fuzzing el cual consiste en conseguir mediante una entrada aleatoria, errores no controlados y explotarlos; el software Metasploit ha introducido del término de “carga útil”, el cual consiste en una base de datos de ataques conocidos, como “webcam peeker” o “drone botnet”, los cuales se utilizan para verificar la seguridad.

3.3 PRINCIPALES CIBERATAQUES Y SUS CONSECUENCIAS

Los ciberataques se realizan casi todos los días, (al menos intentos), por lo general son realizados por personas que tienen cierto conocimiento del sistema a ingresar ilegalmente, aunque en otros casos son los administradores del sistema.

En cualquier caso, los ataques pueden ser por personas o grupo de personas externas, así como internas, siendo los motivos diversos, desde aplicar “justicia” hasta mostrar la capacidad tecnológica que se posee. Sin importar las causas o causales, es claro que ante la ley toda intrusión sin consentimiento o autorización de la empresa o gobierno será considerado ilegal y como consecuencia será catalogado como responsable(s) de un ciberataque y dependiendo del país, esto puede derivar en cárcel, multa o ambas.

Los ciberataques de mayor impacto en la historia reciente son [13]:

Ataque del Departamento de Asuntos de Veteranos de EEUU: en mayo del 2006, los datos personales de 26,5 millones de veteranos, personal activo militar y sus familias, fueron tomados y luego encontrados en una laptop y disco externo obtenidos de un robo previo. El gobierno de EEUU indicó que la información fue recuperada pero los costos de prevención de incidentes podrían llegar a unos 500 millones de dólares. Un desconocido entregó el disco duro donde se encontraba la base de datos el 29 de junio del 2006; aunque el FBI realizó la investigación del caso, no hubo detenidos.

Ataque a AOL: el 6 de agosto del 2006, los datos de 650.000 usuarios, incluida información bancaria y compras, fueron revelados públicamente en un sitio web; esto se debió a que el Dr. Abdur Chowdhury concentró la información de búsquedas de tres meses realizadas por los usuarios en un archivo de texto comprimido con fines de investigación, pero fue publicado por error por AOL, esto llevó a la renuncia del Director de Tecnología Maureen Govern el 21 de agosto del 2006.

Ataque a Heartland Payment Systems: en marzo del 2008, la base de datos del Heartland Payment Systems, sufrió un ataque, el cual tuvo como consecuencia la exposición de 134 millones de tarjetas de crédito y débito. Luego, Albert Gonzales, fue hallado culpable del delito y sentenciado a 20 años en una prisión federal.

Ataque del gobierno Chino a compañías: en el 2009, el gobierno Chino, lanzó un ataque masivo sin precedentes contra docenas compañías de Silicon Valley, California EEUU, entre ellas, Yahoo y Google, esta última confesó que algunos datos de su propiedad intelectual fueron sustraídos, así como datos de activistas chinos de derechos humanos. De parte de Google, se anunció que sus operaciones en China cesarían en el futuro.

Los ataques mencionados han sido efectuados por personas externas, lo que también se conoce como “Ataque Malicioso”; sin embargo, los ataques también son perpetrados, por personas internas, es decir, desde dentro del sistema. Un ejemplo:

Ataque a Fidelity National Information Services: en julio del 2007, un empleado, robó 3.2 millones de registros de clientes, incluidos los datos bancarios, tarjetas de crédito e información personal, los cuales fueron vendidos a intermediarios y a su vez a otras empresas, después de una demanda contra Fidelity National Information Services, el DBA, William Sullivan se declaró culpable del cargo de fraude federal y fue sentenciado a cuatro años y nueves meses de cárcel y pagar una multa de 3.2 millones de dólares.

Las consecuencias de los ataques informáticos (ciberataques) no solo son económicos o de privación de libertad, sino de una perdida de reputación y confianza del público hacia las empresas o gobiernos víctimas de los ciberataques, y estas pueden llegar a la desaparición, ya que, si la confianza no existe entre los clientes y las empresas de servicios, estos migran sus operaciones hacia otros proveedores que si le cumplan con la confidencialidad de sus datos.

3.4 IMPACTO CULTURAL DEL HACKING (CRACKING)

El término “Hacker” surgió en la década de los 1960 en el MIT (Massachusetts Institute of Technology), los cuales fueron un grupo de personas que trabajaban en el laboratorio de inteligencia artificial para realizar ciertas bromas o juegos a los que denominaban “hacks” (por conclusión, la persona que realizaba los hacks, se autodenominaba “hacker”).

Los hackers son entusiastas o expertos en programación e informática que han dedicado muchas horas en la creación de software libre, ya sea para el ámbito empresarial o casero. Gracias a ellos se dispone de los sistemas operativos Unix (Bell Labs), Linux (más sus variantes); Internet (antes Arpanet), el cual lo globalizaron para tener un medio de comunicación más eficiente y de mayor velocidad que la telefonía tradicional; la patente de licencias GNU, el cual todo software realizado bajo esta licencia es de libre uso (incluso su código fuente) para cualquier persona que así lo desee, siempre y cuando, se otorgue el crédito respectivo por su creador.

Así como los hackers han dado muchos beneficios a la comunidad, también han existido quienes han utilizados sus conocimientos para cometer delitos (ahora

conocidos con términos como ciberdelincuentes, ciberterroristas), generando virus (gusanos, troyanos), descarga ilegal de información de entidades públicas y privadas, intrusión en sistemas corporativos o gubernamentales para robo de información o indisponer los servicios.

Durante la mitad de los años 1990 se realizó una separación entre expertos informáticos y delincuentes informáticos. Los primeros fueron los llamados hackers y los segundos catalogados como crackers. Al pasar los años y la masificación de la tecnología como medio de vida, ahora resulta poco asertivo esa clasificación en lo que ha derivado en la denominada “Cultura Hacker”, la cual nace de una sociedad que está conectada todo el tiempo (always online). A manera de activismo tienen como objetivo el cambio del estilo de vida, terminar con la desinformación de los medios de comunicación masivos (depende de la perspectiva), liberación del conocimiento para la población, pero para conseguir esto muchas veces se basan en actos ilegales.

Dentro de la cultura hacker se tienen algunas clasificaciones de grupo de personas, que de acuerdo a sus capacidades pueden caer en las designaciones mostrados en la figura 3.1:

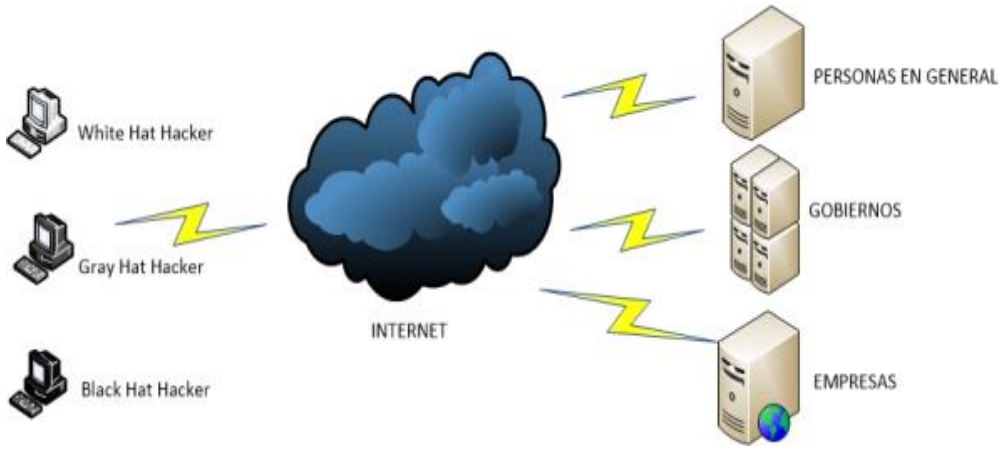


Figura 3.1 Clasificación de hackers

- **Black hat Hackers:** Son ciberdelincuentes que dedican sus esfuerzos para lucrarse a través del robo de información (de empresas o entidades financieras), fraude bancario (compras con tarjetas de crédito,

transferencias ilegales, depósitos en cuentas no autorizadas), indisponibilidad de servicios por diversión.

- **Gray Hat Hackers:** Son iguales a los Black Hat Hackers, pero su diferencia radica en que detectan fallos en los sistemas en empresas mediante una intrusión ilegal para luego ofrecer sus servicios y reparar los daños.
- **White Hat Hackers:** Son personas que generalmente se encuentran en el mundo de la seguridad informática, es decir, poseen igual conocimiento de *Hacking,* pero lo utilizan para blindar los sistemas de acceso.

Existen personas que se sienten atraídas por este mundo. El mundo del cine y entretenimiento muchas veces ha exagerado y alabado este tipo de actos ilegales.

Es tanto el impacto mediático, que las personas con poco o nulo conocimiento en informática se adentran en portales web y descargan software que aparentemente le ayudarán a *"hackear"* correos electrónicos, cuentas de redes sociales, accesos a bancas virtuales y demás, sin saber que no existe software específico que realice un *"hackeo"* de los servicios mencionados, sino que es un conjunto de técnicas y programas varios que se utilizan para la explotación de las vulnerabilidades conocidas.

CAPÍTULO 4

4. PLAN DE CONTINGENCIA ANTE CIBERATAQUES, CÓMO Y POR QUÉ

Los planes de contingencia son importantes para salvaguardar la integridad de la información de las empresas o entidades públicas, en este caso, ante un ciberataque que compromete el sistema y pueden existir filtrado de archivos o documentos confidenciales, en el presente capítulo se expondrán los diferentes planes de contingencia que existen, sus definiciones y la importancia que tienen esta clase de proyectos.

4.1 Planes de contingencia y sus definiciones

Los planes de contingencia en los actuales momentos deben ser considerados imprescindibles, ya que los servicios o el negocio no pueden detenerse porque incurrirían en pérdida de dinero.

El estado ecuatoriano, a través de la Secretaría Nacional de la Administración Pública (SNAP), ha generado directrices para la Seguridad de la Información. Sin embargo, a nivel público o privado no se tiene un plan de continuidad del negocio que también tenga un plan de respuesta a Ciber Incidentes (CIRP, por sus siglas en inglés). Lo único que se ha implementado han sido sitios alternativos ante un desastre (natural o provocado por el hombre).

Se define como “Plan de Contingencia” a una serie de procesos alternos a la normal operación de una empresa o institución, con la finalidad de continuar con su funcionamiento ante algún tipo de incidente interno o externo. Dentro de este concepto, se debe clasificar por tipos, ya que los planes de contingencia en general llegan a una misma meta, que es salvaguardar la información y la continuidad del negocio. Sus causales y metodologías son distintas.

Los tipos de planes de contingencias se mencionan a continuación:

- **Plan de Continuidad del Negocio:** Este tipo de plan asegura las funciones comerciales de una empresa durante y después de la

interrupción de forma básica, mas no contempla una recuperación a largo plazo.

- **Plan de recuperación del negocio:** Este tipo de plan se asegura la restauración de los procesos después de una emergencia (desastre), pero no contempla la continuidad del negocio durante el evento de desastre.
- **Plan de Continuidad de Operaciones:** Este tipo de plan se asegura en la restauración de procesos críticos en un sitio alterno hasta 30 días antes de regresar a las operaciones normales, pero no contempla interrupciones menores.
- **Plan de Comunicaciones ante Crisis:** Este tipo de plan asegura que la información hacia el público, interno o externo será llevado por un grupo de personas autorizadas a rendir una versión oficial sobre los hechos. Este tipo de plan es siempre un anexo de otros planes.
- **Plan de Respuesta ante Ciber Incidentes:** Este tipo de plan establece las directrices a seguir ante ciberataques. Este procedimiento guía al personal de seguridades de la institución a identificar, mitigar y restablecer los sistemas informáticos ante intrusiones ilegales, caída de servicios, o fallos en la infraestructura tecnológica. Así mismo, los identifica como los únicos autorizados para realizar declaraciones sobre los incidentes ocurridos, sus causas y soluciones temporales y a largo plazo.
- **Plan de Recuperación de Desastres:** Este tipo de plan establece el procedimiento a seguir ante grandes desastres que afecten la operación normal por un largo período, debiendo utilizar un sitio alterno después de la emergencia. Este plan no responde a interrupciones menores del sistema.
- **Plan de Emergencia Ocupacional:** Este tipo de plan establece los procedimientos que se deben seguir ante una emergencia por los ocupantes (personal) en caso de alguna amenaza interna o externa.

Existen muchos tipos de planes de contingencia que son utilizados de acuerdo a las necesidades de las instituciones, incluso pueden combinarse para tratar de

cubrir la mayor cantidad de eventos y mitigar las pérdidas de información por daño en almacenamientos, dinero por indisponibilidad de servicios, filtración de información hacia el público que puede provocar inestabilidad en los clientes o usuarios.

El plan de contingencia que se utilizará es una combinación de **"Plan de respuesta ante Ciber Incidentes"**, **"Plan de Recuperación de Desastres"** y **"Plan de Continuidad del Negocio"** y establecerá una guía general para aplicarse en instituciones públicas y privadas.

4.2 Aspectos generales para desarrollar un plan de contingencia

Los planes de contingencia deben desarrollarse primero considerando los aspectos generales y luego los aspectos específicos, esto es, establecer una metodología, normas internaciones aplicables y dependiendo del tipo de negocio que las instituciones posean, alinearse con las leyes locales para evitar problemas legales (instituciones privadas y públicas) y cumplir con las planificaciones anuales (instituciones públicas).

Los planes de contingencia deben ser planificados, ejecutados y mantenidos en el tiempo como proyectos, con sus respectivos acuerdos de mejoras y mantenimientos programados los pasos básicos que deben tomarse en cuenta para su desarrollo son:

- Definición
- Planificación
- Realización
- Cierre

La **Definición** debe comenzar con una compresión clara de la meta a alcanzar, primero estableciendo los objetivos que se desean cumplir, por ejemplo: "ante un evento, evitar pérdida de información", "continuar con las operaciones del negocio, dentro de un tiempo establecido", "ante ataques internos o externos, operar en un sitio alterno, propio o alquilado".

La **Planificación** debe establecer qué tipo de planes de contingencia satisfacen los objetivos definidos y mediante un grupo de personas autorizadas se deben trazar la metodología a seguir para la recuperación de los procesos críticos, evitar alteraciones en la información almacenada, rendir una versión oficial del evento y socializarla con el personal interno y externo (si fuera el caso) para de esta forma impedir rumores que deriven en desconfianza en la institución y continuidad del negocio a corto y largo plazo, asumiendo un riesgo controlado con un tiempo de indisponibilidad de servicio muy reducido. En esta etapa se debe tomar en cuenta los fallos que no pueden ser controlados por la institución (cortes de energía abruptos, cortes de fibra óptica, manifestaciones sociales violentas, eventos naturales o provocados por el hombre, ataques informáticos, entre otros).

La **Realización** conlleva la parte principal de todo el plan, ya que es la ejecución de toda la etapa de planificación, se detectarán los errores y se realizarán los ajustes necesarios para que el plan de contingencia sea lo más eficiente posible al momento de un evento y se lleva a cabo lo siguiente:

- Se especifican los requisitos de las diferentes unidades o departamentos de la institución y se establecen sus prioridades.
- Se analiza y evalúa el proceso de recuperación mediante un plan determinado.
- Se determina el proceso de recuperación.
- Se realizan pruebas de los procedimientos y plan de recuperación.

El **Cierre** debe contemplar la aceptación formal del plan de contingencia propuesto, probado y corregido, por parte de la administración de la institución y personal que se encargará de la ejecución del plan ante cualquier eventualidad.

El trabajo de planificación no solo se centra en la creación de un documento guía, sino que debe coordinar el conjunto de recursos que será la infraestructura del plan de contingencia. Para ello se necesita un **lugar para control**, un **sitio alterno** con equipos y **almacenamiento de datos** suficiente o igual al principal para operar desde unas horas hasta un tiempo indefinido, esto es, hasta cuando termine el proceso de recuperación.

El centro de control no puede centralizarse en un solo lugar, ya que si la edificación queda inaccesible no se podrá ejecutar el plan de contingencia. Por eso es necesario tener al menos un centro de control alterno para ejecutar el plan de contingencia, pudiendo ser un lugar cerca la institución o una sucursal.

El sitio alterno es un lugar con iguales características al sitio principal, donde la institución empezará a funcionar durante el evento. Existen algunas definiciones de sitios alternos, como sitio “espejo”, “caliente”, “frio” y “móvil”. De acuerdo a las necesidades actuales, los sitios “calientes”, “frio” están en desuso porque su funcionamiento implica indisponibilidad de servicio por horas y a veces hasta días. El sitio “móvil”, está orientado para eventos de guerra o desastres de índole nacional, donde los diferentes estados pueden dirigir sus operaciones electrónicas desde cualquier punto del país, esto conlleva a grandes inversiones de dinero.

El sitio alterno que se acopla a la mayoría de las exigencias actuales es el sitio “espejo”, donde las instalaciones principales y alternas tiene una comunicación permanente y sus datos se encuentren sincronizados, permitiendo que ante un evento el funcionamiento del sitio alterno sea prácticamente inmediato.

La aplicación del sitio espejo no excluye la realización de respaldos de información de los servidores (sistemas operativos, aplicaciones), bases de datos e información de los usuarios de las computadoras que utilizan, ello para evitar pérdida de información, ya sea por error humano o fallos de hardware. Estos respaldos pueden ser almacenados en Centros de Datos más grandes a manera de nube, almacenamiento de alta gama (Hitachi, Netapp, etc) o en cinta magnética, esta última no es muy popular ya que para salvaguardar la información se deben realizar copias de seguridad de las cintas, incurriendo en presupuestos mayores de compra de insumos.

El tipo de respaldo más utilizado actualmente es el almacenamiento en Centros de Datos grandes con certificación TIER III ó IV. De acuerdo a un contrato de servicios, no existirá pérdida de información y la administración de los servidores dedicados al almacenamiento de datos son administrados por el proveedor del

servicio sin incurrir en gastos adicionales de lo acordado en el contrato. Los tipos de centros de cómputo se muestran en la figura 4.1:

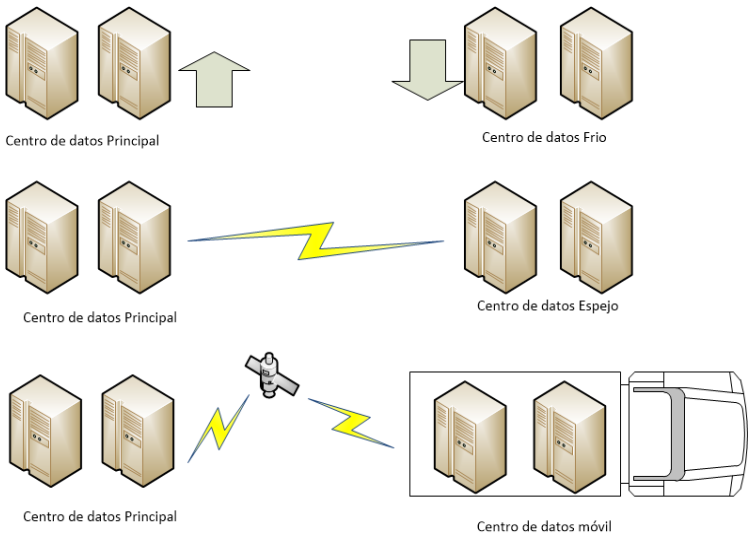


Figura 4.1 Tipos de Centros de Datos alternos

4.3 Disponibilidad de servicios en un mundo conectado a la red

Las personas actualmente realizan sus actividades con el apoyo de computadoras, celulares, tablets y cualquier otro dispositivo que tenga conexión a Internet, donde no solo se emplean para trabajar tradicionalmente (correo electrónico, llamadas, mensajería), sino también son utilizados para el ocio (redes sociales, noticias al instante, marketing de productos), y últimamente, para gestionar algún tipo de negocio que generalmente incurre en la venta de productos propios, re-vender productos de algún fabricante no necesariamente dentro del país, sino de algún lado del mundo u ofrecer servicios para PYMEs.

Este tipo de evolución de trabajo también dinamiza la economía, donde los pagos e ingresos de forma tradicional, aun en vigencia, de instituciones financieras, centros comerciales, locales de comida, ropa y demás, incurran en el mundo de conectividad global. Los tipos de negocios están evolucionando no solo en la forma de pago de servicios, sino en establecer y hasta mudar operaciones donde no se necesite una infraestructura propia para disminuir costos. Un ejemplo es el portal www.prosper.com, que es un banco no

tradicional, donde los usuarios pueden conectarse sin intermediarios para realizar préstamos de dinero a personas naturales o jurídicas pudiendo negociar las tasas de interés y el tiempo de pago, también realizar operaciones con criptomonedas, aunque el más popular es el Bitcoin, existen otras como el Litecoin, Ethereum, Ripple, Dogecoin, entre otras, las cuales tienen sus ventajas y desventajas y son una opción al dinero tradicional; este tipo de monedas están bajo observación legal en la mayoría de los países, ya que son utilizadas para estafas en la red.

El portal www.thredup.com, conecta a padres de familia para intercambiar ropa de sus hijos en buen estado cuando ya crecen en lugar de comprar ropa nueva. El portal www.zipcar.com, ofrece un servicio para compartir el auto, donde por un precio muy bajo se puede utilizar un auto hasta por 8 horas y luego liberarlo para que otro usuario lo utilice, esta iniciativa nació de personas que no necesitan comprar un auto si solo lo utilizan 2 horas al día.

Los ejemplos citados son servicios que ya se ofrecen vía conexión a la red. Partiendo de este argumento, el sistema que está detrás de los servicios ofrecidos y utilizados no pueden tener una interrupción prolongada, ya que afectan los negocios alojados y gestionados y conllevaría a una pérdida económica y malestar en el cliente, generando desconfianza y búsqueda de una alternativa. Un ejemplo de este tipo de evento fue la caída que sufrió el servicio WhatsApp el 22 de febrero del 2014, oficialmente (informado a través de twitter) atribuido a un fallo en los servidores por algunas horas, provocando que los usuarios migren hacia el servicio Telegram como red social alternativa.

Este simple ejemplo, indica que la disponibilidad de servicios en la actualidad deber ser sin interrupciones. Por ello, de manera obligatoria se debe poseer un plan de contingencia de sitio espejo para que los usuarios no experimenten fallos en los servicios o al menos la interrupción sea de unos pocos minutos, a manera de microcorte, e informar de manera eficiente y formal el evento hacia los clientes y público en general. La disponibilidad de servicios informáticos, sin importar su naturaleza, debe ser parte de la misión de las empresas e instituciones públicas en un mundo conectado a la red.

CAPÍTULO 5

5. DESARROLLO DE LA ESTRATEGIA

En el presente capítulo se expondrá el desarrollo de la estrategia escogida, para ello se definirán la prioridad de los servicios, luego planificando el plan de contingencia y se escoge una estrategia mediante un análisis económico de tener un sitio alterno propio o en la nube.

5.1 Definición de servicios según su prioridad

Los servicios tecnológicos ofrecidos por empresas o instituciones gubernamentales son muy variados, desde ventas de cualquier producto (terminado o materia prima), pasando por la atención al público, hasta contemplar necesidades de cualquier índole que las personas requieran, como por ejemplo: alimentación, transporte, comunicación, pagos de facturas, tramites gubernamentales, entre otros.

Los servicios que serán materia de análisis son los de carácter financiero, en la rama de compra/venta de productos tangibles o intangibles que se realicen mediante tarjetas de crédito o débito.

El datacenter de la empresa que quiera incursionar en la intermediación entre el banco y el cliente, para el procesamiento de transacciones de tarjetas de crédito y débito de forma electrónica en tiempo real, debe poseer al menos los siguientes equipos:

- Directorio activo (windows server 2012)
- Correo Office 365
- Base de datos SQL SERVER (SQL SERVER 2010)
- Sistema de telefonía voip para usuarios y servicio al cliente (2 servidores con elastix 2.5 instalado).
- Servidor dedicado para Storage.
- Servidor de facturación electrónica (centos 6.8)
- Servidor de registros de pagos (windows server 2012)

- Librería HPE StoreEver MSL4048 0-drive Tape
- Equipos de comunicación: switch, routers cisco y Firewalls checkpoint

La lista de equipos mencionada solo debe considerarse como una referencia de la infraestructura básica para las operaciones de un Datacenter, ya que los mismos son variables de acuerdo al presupuesto de la empresa y sus necesidades reales.

Los servicios prioritarios y no prioritarios son ofrecidos a través de equipos informáticos y de comunicación, por lo tanto, la disponibilidad de servicios se traduce como disponibilidad del equipo que lo ofrece.

El diseño presentado es un esquema básico de conexiones y se pueden diferenciar las prioridades de los equipos.

Los equipos de prioridad alta son:

- Equipos de comunicación (switch, routers, firewalls).
- Servidor de Base de datos SQL SERVER.
- Servidor de registro de pagos
- Servidor Storage

Los equipos de prioridad media son:

- Servidor de Directorio activo
- Servidor de Correo Exchange
- Servidores Elastix
- Servidor y Libreria HPE StoreEver MSL4048 0-drive Tape
- Servidor de facturación electrónica

Los equipos de prioridad baja son los equipos de usuarios de la empresa.

Las estaciones de trabajo de jefaturas, gerencias, operadores del Datacenter y el personal que se considere indispensable para las operaciones normales de la empresa, tendrán una réplica en el centro de control alterno.

5.2 Planificación de un plan de continuidad

La planificación de un plan de continuidad es un proceso importante en las empresas de la actualidad, ya que les permitirá continuar con el negocio sin afectación de los servicios o al menos una intermitencia de corta duración. Los tipos de planes son muy variados y se establecen de acuerdo a las necesidades de las empresas o instituciones públicas. Para el caso de una empresa con tipo de negocio en el área financiera, los planes a tener en cuenta no solo deben contemplar la continuidad del negocio, sino ante los ataques cibernéticos, que son ejecutados a través de virus, intrusiones ilegales, saturaciones anormales de enlaces de datos, caída de equipos de comunicación y servidores.

El plan de continuidad que puede abarcar las necesidades de una empresa de ámbito financiero, como tal, no existe, sino que es una combinación de dos o más tipos de planes, en este caso, la base deben ser los planes:

- **Plan de Continuidad del Negocio:** Este tipo de plan asegura las funciones comerciales de una empresa durante y después de la interrupción de forma básica, mas no contempla una recuperación a largo plazo.
- **Plan de Respuesta ante Ciber Incidentes:** Este tipo de plan establece las directrices a seguir ante ciberataques. Este procedimiento guía al personal de seguridades de la institución a identificar, mitigar y restablecer los sistemas informáticos ante intrusiones ilegales, caída de servicios, o fallos en la infraestructura tecnológica. Así mismo, los identifica como los únicos autorizados para realizar declaraciones sobre los incidentes ocurridos, sus causas y soluciones temporales y a largo plazo.

Las combinaciones de los planes listados permitirán garantizar la operatividad de la empresa y por extensión los servicios ofrecidos hacia los clientes o público en general, para asegurar la continuidad del negocio ante ciberincidentes, contemplando la indisponibilidad solo ante pequeños eventos.

El plan de continuidad o contingencia tendrá los siguientes objetivos:

- Disponibilidad de los servicios el 95% del tiempo [12], ante cualquier evento.
- Poseer un sitio alterno (propio o en la nube) que contenga equipos iguales o virtualizados del Data Center.
- Establecer un centro de control alterno para gestionar levantamiento de la contingencia.
- Generar un procedimiento de acción para personal de seguridades ante un ciberincidente.
- Utilizar los recursos tecnológicos más convenientes para mitigar los ciberincidentes.

Los objetivos trazados en general garantizarán una operatividad de poco impacto (indisponibilidad de unos minutos) hasta que el sistema alterno se encuentre con la información actualizada y online ante un desastre provocado por un ciberincidente. La respuesta se puede dar en dos escenarios: subiendo el sitio alterno en caso de que el centro principal sufra un daño en un equipo a consecuencia del ciberincidente o en el mismo centro de datos principal si el evento se puede aislar en cuestión de minutos.

El aislamiento de los incidentes se realiza mediante técnicas de detección y prevención avanzadas desplegadas en equipos (appliance) de reconocidas marcas dedicadas a la ciberseguridad. Estos equipos no son infalibles, pudiendo ser en algún momento vulnerados, ya que los ataques constantemente están mutando y mejorando para romper las seguridades de los sistemas; por lo tanto, siempre se debe contar con personal con conocimientos en tecnologías de la información especializado en seguridad informática para analizar los comportamientos del tráfico de red, aumentos de consumo de ancho de banda, revisión de los portales, web de acceso público, generar y estudiar reportes de los equipos encargados de la seguridad de la red para establecer patrones de tráfico tanto internos como externos y realizar auditorías regulares sobre las actividades de los usuarios internos en el uso de los recursos brindados por la empresa (navegación web, correo electrónico, uso de dispositivos externos, posibles infecciones de virus, entre otros).

La planificación que se podría realizar para cumplir los objetivos trazados son:

- Levantar un sitio alterno, propio o en la nube.
- Asilar el evento con recursos tecnológicos modernos.

5.3 Escoger una estrategia

La estrategia a escoger debe basarse en un análisis financiero sobre el almacenamiento de un sitio propio y la virtualización de los servicios, luego debe pasar un análisis técnico para establecer el parque tecnológico necesario, por último, se debe decidir por la mejor opción tanto en presupuesto como en tecnología.

El análisis técnico en este caso es basado en una comparación entre la construcción de un sitio alterno o virtualización en la nube a nivel financiero, ya que tecnológicamente ambos escenarios son confiables y viables, pero no debemos descuidar el presupuesto asignado y no sobrepasar los límites de gastos de la empresa, ya que puede generar problemas económicos en el futuro.

El estudio de costos realizado está basado parcialmente en el capítulo 8 del proyecto de titulación "**ESTUDIO PARA IMPLEMENTACIÓN DE SERVICIOS DE DATACENTER BASADOS EN EL MODELO CLOUD COMPUTING**, cuya autoría corresponde a Augusto Cabrera. Sin embargo, el presente análisis está orientado hacia el negocio de una empresa de servicios financieros (explicada en el capítulo 6), donde su negocio es la recaudación de pagos de todos los servicios (básicos, especiales) y de empresas pequeñas y medianas (PYMES), así como de personas con un RUC registrado.

El primer análisis realizado será de la construcción de un sitio alterno con todo lo necesario para su óptimo funcionamiento. El segundo análisis será de la virtualización de equipos en la nube. En ambos escenarios habrá que comprar equipos dobles que por sus características no puedan ser virtualizados y deban obligadamente ocupar un espacio físico.

Primeramente, se debe tener claro los tipos de costos a tomar en cuenta:

- **Costos directos:** Son los costos relacionados directamente con el servicio.
- **Costos Indirectos:** Son aquellos que no guardan relación directa con el servicio.
- **Costos fijos:** Son aquellos que son independientes al volumen de producción.
- **Costos Variables:** Son aquellos costos que dependen directamente del volumen de producción.
- **Costos de Capital:** Son aquellos que proceden de amortizaciones o inversiones a largo plazo.
- **Costos de operación:** Son aquellos relacionados a los procesos diarios (funcionamiento del dia a dia).

Una vez explicados los tipos de costos que existen, se puede analizar el costo de la construcción de un Data Center alterno, el cual tendrá que estar disponibles 24x7. Para esto, los activos fijos son amortizados, según su característica, entre 5, 10 y 20 años.

Análisis de construcción centro de datos alterno

Los valores de la construcción del centro alterno son referenciales, tomando en cuenta el consumo por rack y los implementos necesarios para climatización, respaldo de energía y equipos necesarios (servidores, racks).

Los servidores son tipo rack, de características similares al centro de datos principal, están listos para entrar en operaciones ante una eventual activación de contingencia. Los racks son tipo gabinete de 19U (unidades) de puertas perforadas (ambas puertas) para climatización, Aires de Precisión, sistema contra incendios, elementos para construir la red (jacks, conectores, cable UTP cat 6A, fibra óptica, etc).

El respaldo de energía se compone de UPS y generador trifásico. La alimentación principal siempre será la otorgada por las líneas de alta tensión de la empresa eléctrica estatal, pasando por transformadores (propios), inversores y paneles eléctricos industriales.

La climatización estará a cargo de los aires de precisión, ya que estos equipos no solo se encargan de enfriar el ambiente, también poseen sensores de humedad, líquidos, sequedad del ambiente y se autorregulan para asegurar una operación normal de equipos informáticos y sin congelarse como los aires acondicionados de confort. La figura 5.1 muestra los tipos de planes de contingencia utilizados y los costos que conllevan implementarlos y a figura 5.2 indica los equipos a instalarse en el Centro de Datos alterno:

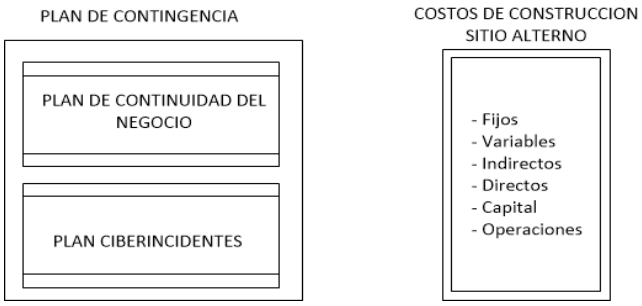


Figura 5.1 Tipos de planes y costos para centro de datos alterno

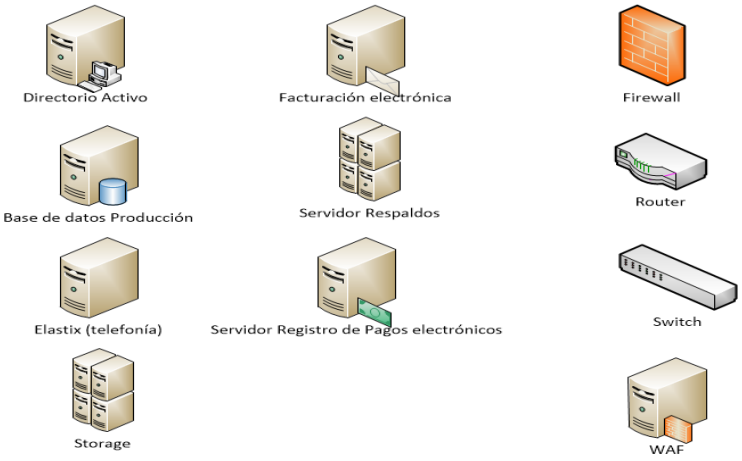


Figura 5.2 Equipos a instalarse en el Centro de Datos alterno

La tabla 1 muestra la proyección a 5 años de los costos de construcción de un Centro de Datos alterno. Las tablas 2 al 6, muestran las proyecciones por costos de remuneraciones de personal que administrará el Centro de Datos secundario y la tabla 7 muestra un resumen de las remuneraciones anuales, las cuales se muestran a continuación:

Los valores aproximados del centro de datos alterno son[*]:

ANALISIS DE COSTOS DATACENTER SECUNDARIO					
	2017	2018	2019	2020	2021
INVERSION					
Transformador, acometida	$ 25.200,00				
Generador	$ 150.000,00				
Baterías (para generador)	$ 500,00				
Rectificador	$ 80.000,00				
Edificio	$ 250.000,00				
Climatización	$ 2.500,00				
Sistema contra incendios	$ 6.000,00				
Racks	$ 200,00				
Canaletas, Escalerillas	$ 1.500,00				

[*] Costos basados en experiencia del autor.

Conexión a Tierra	$ 5.000,00				
Servidores	$ 50.000,00				
Servidor STORAGE	$ 3.000,00				
Sistemas de respaldos	$ 4.000,00				
Equipos de Comunicación	$ 3.000,00				
TOTAL DE INVERSION	**$ 580.900,00**	$ 0,00	$ 0,00	$ 0,00	$ 0,00
Costos operativos y mantenimiento					
Personal de Centro de Datos	$ 90.301,05	$ 94.760,60	$ 99.443,13	$ 104.359,79	$ 109.522,28
Energia eléctrica de Centro de Datos	$ 8.400,00	$ 8.400,00	$ 8.400,00	$ 8.400,00	$ 8.400,00
Póliza de seguros	$ 260.000,00	$ 260.000,00	$ 260.000,00	$ 260.000,00	$ 260.000,00
TOTAL COSTOS	**$ 358.701,05**	**$ 363.160,60**	**$ 367.843,13**	**$ 372.759,79**	**$ 377.922,28**
TOTAL	**$ 939.601,05**	**$ 363.160,60**	**$ 367.843,13**	**$ 372.759,79**	**$ 377.922,28**

Tabla 1 Costos de implementación Datacenter secundario

[*] Costos basados en experiencia del autor.

PERSONAL	REMUNERACION 2017								
	SUELDO	INCREMENTO 5%	MESES	SUELDO ANUAL	APORTE AL IESS (ANUAL)	DECIMO TERCER SUELDO	DECIMO CUARTO SUELDO	FONDO DE RESERVA	TOTAL
Soporte	$ 2.800,00	$ 2.940,00	12	$ 35.280,00	$ 3.933,72	$ 2.940,00	$ 358,00	$ 3.333,96	**$ 51.597,68**
Ing. Infraestructura	$ 1.700,00	$ 1.785,00	12	$ 21.420,00	$ 2.388,33	$ 1.785,00	$ 358,00	$ 2.024,19	**$ 31.472,52**
Seguridad (GUARDIA)	$ 375,00	$ 393,75	12	$ 4.725,00	$ 526,84	$ 393,75	$ 358,00	$ 446,51	**$ 7.230,85**

Tabla 2 Proyección de remuneraciones de personal 2017

PERSONAL	REMUNERACION 2018								
	SUELDO	INCREMENTO 5%	MESES	SUELDO ANUAL	APORTE AL IESS (ANUAL)	DECIMO TERCER SUELDO	DECIMO CUARTO SUELDO	FONDO DE RESERVA	TOTAL
Soporte	$ 2.940,00	$ 3.087,00	12	$ 37.044,00	$ 4.130,41	$ 3.087,00	$ 358,00	$ 3.500,66	**$ 54.159,06**
Ing. Infraestructura	$ 1.785,00	$ 1.874,25	12	$ 22.491,00	$ 2.507,75	$ 1.874,25	$ 358,00	$ 2.125,40	**$ 33.027,65**
Seguridad (GUARDIA)	$ 393,75	$ 413,44	12	$ 4.961,25	$ 553,18	$ 413,44	$ 358,00	$ 468,84	**$ 7.573,89**

Tabla 3 Proyección de remuneraciones de personal 2018

PERSONAL	REMUNERACION 2019								
	SUELDO	INCREMENTO 5%	MESES	SUELDO ANUAL	APORTE AL IESS (ANUAL)	DECIMO TERCER SUELDO	DECIMO CUARTO SUELDO	FONDO DE RESERVA	TOTAL
Soporte	$ 3.087,00	$ 3.241,35	12	$ 38.896,20	$ 4.336,93	$ 3.241,35	$ 358,00	$ 3.675,69	**$ 56.848,52**
Ing. Infraestructura	$ 1.874,25	$ 1.967,96	12	$ 23.615,55	$ 2.633,13	$ 1.967,96	$ 358,00	$ 2.231,67	**$ 34.660,53**
Seguridad (GUARDIA)	$ 413,44	$ 434,11	12	$ 5.209,31	$ 580,84	$ 434,11	$ 358,00	$ 492,28	**$ 7.934,09**

Tabla 4 Proyección de remuneraciones de personal 2019

PERSONAL	REMUNERACION 2020								
	SUELDO	INCREMENTO 5%	MESES	SUELDO ANUAL	APORTE AL IESS (ANUAL)	DECIMO TERCER SUELDO	DECIMO CUARTO SUELDO	FONDO DE RESERVA	TOTAL
Soporte	$ 3.241,35	$ 3.403,42	12	$ 40.841,01	$ 4.553,77	$ 3.403,42	$ 358,00	$ 3.859,48	**$ 59.672,44**
Ing. Infraestructura	$ 1.967,96	$ 2.066,36	12	$ 24.796,33	$ 2.764,79	$ 2.066,36	$ 358,00	$ 2.343,25	**$ 36.375,05**
Seguridad (GUARDIA)	$ 434,11	$ 455,81	12	$ 5.469,78	$ 609,88	$ 455,81	$ 358,00	$ 516,89	**$ 8.312,29**

Tabla 5 Proyección de remuneraciones de personal 2020

PERSONAL	REMUNERACION 2021								
	SUELDO	INCREMENTO 5%	MESES	SUELDO ANUAL	APORTE AL IESS (ANUAL)	DECIMO TERCER SUELDO	DECIMO CUARTO SUELDO	FONDO DE RESERVA	TOTAL
Soporte	$ 3.403,42	$ 3.573,59	12	$ 42.883,06	$ 4.781,46	$ 3.573,59	$ 358,00	$ 4.052,45	**$ 62.637,57**
Ing. Infraestructura	$ 2.066,36	$ 2.169,68	12	$ 26.036,14	$ 2.903,03	$ 2.169,68	$ 358,00	$ 2.460,42	**$ 38.175,31**
Seguridad (GUARDIA)	$ 455,81	$ 478,61	12	$ 5.743,27	$ 640,37	$ 478,61	$ 358,00	$ 542,74	**$ 8.709,41**

Tabla 6 Proyección de remuneraciones de personal 2021

PERSONAL	REMUNERACIONES ANUALES				
	2017	**2018**	**2019**	**2020**	**2021**
Soporte	$ 51.597,68	$ 54.159,06	$ 56.848,52	$ 59.672,44	$ 62.637,57
Ing. Infraestructura	$ 31.472,52	$ 33.027,65	$ 34.660,53	$ 36.375,05	$ 38.175,31
Seguridad (GUARDIA)	$ 7.230,85	$ 7.573,89	$ 7.934,09	$ 8.312,29	$ 8.709,41
TOLTAL ANUAL	**$ 90.301,05**	**$ 94.760,60**	**$ 99.443,13**	**$ 104.359,79**	**$ 109.522,28**

Tabla 7 Resumen de remuneraciones anuales

Para el costo total del centro de datos, como se muestra en la tabla 1, en el primer año se toman en cuenta los precios de los elementos para la construcción y las remuneraciones para el cuidado, administración y monitoreo de las instalaciones. Los sueldos, se los incrementa en un 5% anual para cada empleado para en lo posible evitar la rotación de personal (renuncias e ingreso de personal nuevo), ya que eso comprometería las operaciones normales del centro de datos debido a errores cometidos por inexperiencia, como se muestran en las tablas 2 al 6.

Del segundo año hasta el último solo se toman en cuenta los costos operativos y de mantenimiento, como son: Personal del centro de datos, energía consumida por los equipos y el valor de la póliza de seguros de todos los elementos del datacenter, ya que ante algún daño fortuito no se incurría en un gasto adicional, solo se aplicaría el seguro. Para el personal de soporte son consideradas dos personas: el Ingeniero de Infraestructura uno y la seguridad de las instalaciones es mediante una compañía a través de un contrato de prestación de servicios. El incremento anual del 5% es tomado en cuenta para el personal de seguridad porque es el incremento del contrato y la compañía se encargará de gestionarlo entre su personal.

Análisis de Centro de Datos en la nube (virtual)

La oferta de centro de datos virtual actualmente es ofrecida por la compañía CLARO, la cual es líder a nivel de Latinoamérica; sus grandes Centros de Datos los tiene ubicados en distintos países como México, Brasil, Colombia y Argentina, para implementaciones virtuales de Ecuador, se utiliza el Centro de Datos ubicado en la Ciudad Autónoma de Belgrano en Argentina. Las empresas TELCONET y CNT son representantes a nivel local del sector privado y público, respectivamente, y ofrecen servicios de housing, servidores virtuales en sus Centros de Datos, incluso un sistema de respaldos en línea, sin embargo, la figura de Centro de Datos Virtual solo es ofrecida por CLARO, en su centro de datos.

No se necesitan instalaciones físicas para la implementación de un centro de datos alterno con la modalidad virutal (o en la nube) ya que la infraestructura no

depende del cliente (nosotros) sino de la empresa CLARO que ofrece el servicio, a través de su DATACENTER ubicado en la Ciudad Autónoma de Belgrano, en Argentina, el cual opera desde febrero del 2012 y posee certificación TIER 3.

La información procesada y almacenada es garantizada en su integridad y alta disponibilidad gracias a la certificación TIER 3, otorgada por el UPTIME Institute a los Centros de Datos que cumplen los requisitos para ofrecer una disponibilidad del 99.982%, es decir, en un año solo pueden tener interrupciones por 1.6 horas. La figura 5.3 muestra los planes de contingencia aplicados y los costos de alquiler en la nube.

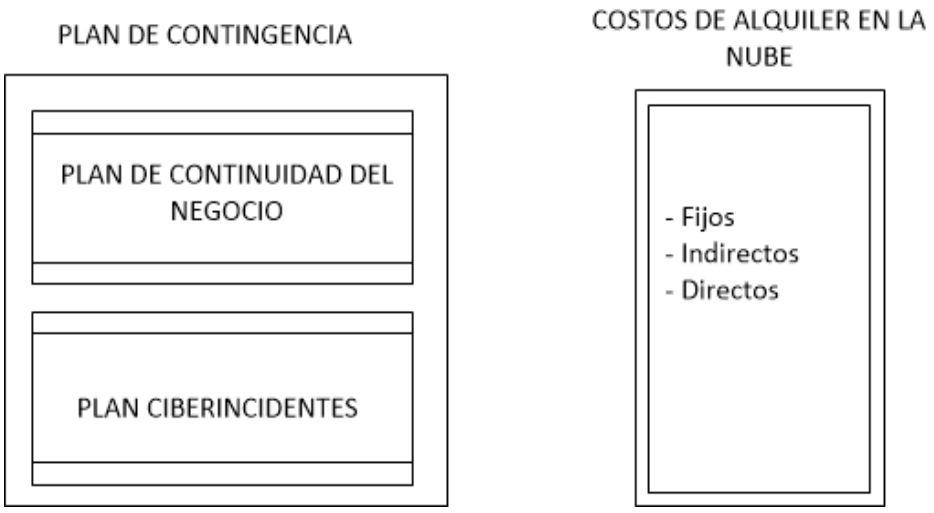


Figura 5.3 Tipos de planes y costos para centro de datos virtual

La tabla 8 muestra la proyección a 5 años de los costos de construcción de un Centro de Datos alterno. Las tablas 9 al 13, muestran las proyecciones por costos de remuneraciones de personal que administrará el Centro de Datos secundario y la tabla 14 muestra un resumen de las remuneraciones anuales. Los costos de operación del Centro de datos alterno en la nube[*], se muestran a continuación:

[*] Costos referenciales tomados del sitio web de Claro Cloud

ANALISIS COSTOS DATACENTER VIRTUAL					
INVERSION	2017	2018	2019	2020	2021
Servidores Windows	$ 1.491,12				
Servidores Linux	$ 1.593,72				
Datacenter Virtual	$ 558,60	$ 558,60	$ 558,60	$ 558,60	$ 558,60
Enlace Dedicado	$ 70,00	$ 70,00	$ 70,00	$ 70,00	$ 70,00
TOTAL INVERSION	**$ 3.713,44**	**$ 628,60**	**$ 628,60**	**$ 628,60**	**$ 628,60**
COSTOS OPERATIVOS					
Administracion de CLOUD	$ 134.297,88	$ 140.975,77	$ 147.987,56	$ 155.349,90	$ 163.080,43
TOTAL	**$ 138.011,32**	**$ 141.604,37**	**$ 148.616,16**	**$ 155.978,50**	**$ 163.709,03**

Tabla 8 Costos de implementación Datacenter virtual

PERSONAL	REMUNERACION 2017								
	SUELDO	INCREMENTO 5%	MESES	SUELDO ANUAL	APORTE AL IESS (ANUAL)	DECIMO TERCER SUELDO	DECIMO CUARTO SUELDO	FONDO DE RESERVA	TOTAL
Soporte	$ 5.600,00	$ 5.880,00	12	$ 70.560,00	$ 7.867,44	$ 5.880,00	$ 358,00	$ 6.667,92	**$ 102.825,36**
Ing. Infraestructura	$ 1.700,00	$ 1.785,00	12	$ 21.420,00	$ 2.388,33	$ 1.785,00	$ 358,00	$ 2.024,19	**$ 31.472,52**

Tabla 9 Proyección de remuneraciones de personal 2017

PERSONAL	REMUNERACION 2018								
	SUELDO	INCREMENTO 5%	MESES	SUELDO ANUAL	APORTE AL IESS (ANUAL)	DECIMO TERCER SUELDO	DECIMO CUARTO SUELDO	FONDO DE RESERVA	TOTAL
Soporte	$ 5.880,00	$ 6.174,00	12	$ 74.088,00	$ 8.260,81	$ 6.174,00	$ 358,00	$ 7.001,32	**$ 107.948,13**
Ing. Infraestructura	$ 1.785,00	$ 1.874,25	12	$ 22.491,00	$ 2.507,75	$ 1.874,25	$ 358,00	$ 2.125,40	**$ 33.027,65**

Tabla 10 Proyección de remuneraciones de personal 2018

PERSONAL	REMUNERACION 2019								
	SUELDO	INCREMENTO 5%	MESES	SUELDO ANUAL	APORTE AL IESS (ANUAL)	DECIMO TERCER SUELDO	DECIMO CUARTO SUELDO	FONDO DE RESERVA	TOTAL
Soporte	$ 6.174,00	$ 6.482,70	12	$ 77.792,40	$ 8.673,85	$ 6.482,70	$ 358,00	$ 7.351,38	**$ 113.327,03**
Ing. Infraestructura	$ 1.874,25	$ 1.967,96	12	$ 23.615,55	$ 2.633,13	$ 1.967,96	$ 358,00	$ 2.231,67	**$ 34.660,53**

Tabla 11 Proyección de remuneraciones de personal 2019

PERSONAL	REMUNERACION 2020								
	SUELDO	INCREMENTO 5%	MESES	SUELDO ANUAL	APORTE AL IESS (ANUAL)	DECIMO TERCER SUELDO	DECIMO CUARTO SUELDO	FONDO DE RESERVA	TOTAL
Soporte	$ 6.482,70	$ 6.806,84	12	$ 81.682,02	$ 9.107,55	$ 6.806,84	$ 358,00	$ 7.718,95	**$ 118.974,89**
Ing. Infraestructura	$ 1.967,96	$ 2.066,36	12	$ 24.796,30	$ 2.764,79	$ 2.066,36	$ 358,00	$ 2.343,25	**$ 36.375,01**

Tabla 12 Proyección de remuneraciones de personal 2020

PERSONAL	REMUNERACION 2021								
	SUELDO	INCREMENTO 5%	MESES	SUELDO ANUAL	APORTE AL IESS (ANUAL)	DECIMO TERCER SUELDO	DECIMO CUARTO SUELDO	FONDO DE RESERVA	TOTAL
Soporte	$ 6.806,84	$ 7.147,18	12	$ 85.766,12	$ 9.562,92	$ 7.147,18	$ 358,00	$ 8.104,90	**$ 124.905,13**
Ing. Infraestructura	$ 2.066,36	$ 2.169,68	12	$ 26.036,14	$ 2.903,03	$ 2.169,68	$ 358,00	$ 2.460,41	**$ 38.175,30**

Tabla 13 Proyección de remuneraciones de personal 2021

PERSONAL	REMUNERACIONES ANUALES				
	2017	2018	2019	2020	2021
Soporte	$ 102.825,36	$ 107.948,13	$ 113.327,03	$ 118.974,89	$ 124.905,13
Ing. Infraestructura	$ 31.472,52	$ 33.027,65	$ 34.660,53	$ 36.375,01	$ 38.175,30
TOLTAL ANUAL	**$ 134.297,88**	**$ 140.975,77**	**$ 147.987,56**	**$ 155.349,90**	**$ 163.080,43**

Tabla 14 Resumen de remuneraciones anuales

El costo total del centro de datos en el primer año, como se muestran en la tabla 8, se toman en cuenta la configuración de los servidores y las remuneraciones para la administración del CDV (Centro de Datos Virtual). Los sueldos se los incrementan en un 5% anual para cada empleado, ya que no solo se encargarían del centro de datos principal, sino que una función adicional seria la administración del CDV, como se muestran en las tablas 9 al 13.

El segundo año hasta el último, solo se toman en cuenta los costos de Administración, alquiler del CDV y el enlace dedicado (conexión de datos hacia el CDV). Las funciones de administración del CDV, básicamente constituyen en actualizar la información de las bases de datos con al menos un dia de retraso, ya que ante cualquier evento, se puede volver a las operaciones normales en cuestión de horas.

El personal técnico encargado del CDV será el mismo que administra el Datacenter principal, por tal motivo, no se incurrirá en gastos de personal adicionales; la infraestructura del Datancenter que aloja el CDV es administrada, gestionada y monitoreada por el proveedor del servicio, la figura 5.4 muestra los equipos informáticos críticos que serán virtualizados.

Figura 5.4 Equipos a virtualizar en Centro de Datos virtual

5.4 Contingencia en la nube

La contingencia en la nube es una opción que ha venido tomando fuerza y forma durante la última década, cuando las empresas grandes empezaban a ofrecer espacio de almacenamiento de información tanto a usuarios finales como a empresas pequeñas y medianas sin que esto genere un costo elevado en la compra de equipos, configuración y administración. Luego empezaron a ofrecer servicios de páginas web, no solo alojarlas, sino mediante herramientas online, construirlas a gusto de cada cliente para ofertar sus productos o simplemente generar información de interés general o hacia un grupo específico.

El concepto de Datacenter Virtual, apareció hace aproximadamente 6 años, pero no fue hasta hace 5 años que, en Latinoamérica, de la mano de Claro (América Móvil), se empezó a ofrecer los servicios en la nube mediante los Datacenter que poseen en Colombia, Argentina, Brasil y México.

La tabla 15 muestra la comparación entre la construcción de un Centro de datos secundario, con el alquiler de un CDV:

Centro de Datos propio	Centro de Datos Virtual
- Mantenimiento de equipos	- Equipos son alquilados
- Costos por administración de centro de datos	- Costo único por configuración
- Personal dedicado al centro de datos secundario	- No requiere personal adicional
- Costo anual por mantenimiento	- Mantenimiento solo depende del proveedor
- Todo el centro de datos debe estar asegurado	- Seguro del centro de datos depende del proveedor
- Inversión realizada solo por medianas y grandes empresas, privadas o estatales.	- Inversión media incluso para PYMES.

Tabla 15 Cuadro comparativo entre centro de datos propio y virtual

El cuadro comparativo da como resultado más viable el Centro de datos virtual, ya que el personal técnico se encarga de gestionar las configuraciones básicas de servidores y demás opciones operativas y administrativas para poner en marcha las funciones de un Centro de datos. La inversión también es un factor importante, en este cuadro podemos ver la diferencia entre la construcción de un Centro de datos y la contratación de un Centro de Datos Virtual (CDV), como se muestra en la tabla 16:

Costos	Datacenter fisico	Datacenter Virtual
Inversión inicial	$ 580.900,00	$3.713,44
Costos operativos (Año 1)	$ 358.701,05	$ 134.297,88
Remuneraciones (Año 1)	$ 90.301,05	N/A
Total costos (Año 1)	$ 939.601,05	$ 138.011,32
Total costos (Año 2)	$ 363.160,60	$ 141.604,37

Tabla 16 Cuadro comparativo de costos entre centro de datos propio y virtual

La inversión inicial de la construcción de un Centro de datos secundario es elevada, en comparación con el CDV, $939.601,05 contra un $138.011,32. En los costos del segundo año en ambos casos se ha considerado el aumento de un 5% en los sueldos por año. Con esto se pretende evitar la rotación de personal frecuente en un área sensible. Un problema a tener en cuenta es la confidencialidad, ya que el temor de mudar operaciones en la nube (principal o como contingencia) es el acceso a la información por personal no autorizado.

Las contrataciones a nivel corporativo, el proveedor y cliente firman un acuerdo de servicio (SLA), confidencialidad y resolución de conflictos sin que afecte la normal operación del CDV o cancelación de servicios unilateralmente en caso de problemas económicos, deber incluirse en el contrato de servicio.

Los acuerdos y condiciones que las empresas publican son generales, es decir, para los usuarios, pero en caso de empresas, estos deben negociar los términos de los contratos y en ellos deben asegurarse de no comprometer la continuidad del negocio.

CAPÍTULO 6

6. SIMULACIÓN DE UN CIBERATAQUE Y REALIZACIÓN DEL PLAN DE CONTINGENCIA

El presente capítulo se expondrá una serie de pasos que van desde el establecimiento de un escenario de desastre típico para una institución financiera para realizar la simulación de un ciberataque, ejecución del plan de contingencia planificado por los equipos humanos involucrados para detectar y detener la amenaza y a su vez el paso desde el ambiente de producción hasta la contingencia, la realización del reverso y una evaluación que determina los fallos de cada equipo y los aspectos a mejorar para mitigar los problemas encontrados y ejecutar de forma óptima el plan de contingencia.

6.1 Escenario de desastre para una institución financiera

Las instituciones financieras, no solo deben considerarse a los bancos y sus sucursales que gestionan fondos de dinero físico de clientes, sino, toda empresa que recepte y procese pagos en línea (paypal, wester unión, solo por mencionar algunas) y procesen transacciones de tarjetas de crédito y débito (Datafast o Banred a nivel local), ya que la información que se administra en estas últimas entidades deben ser tratadas de manera especial, desde el medio de transmisión, pasando por el procesamiento, almacenamiento y destino final de las transacciones que son los bancos y estos a su vez realizan el depósito en las cuentas de los clientes de acuerdo a la información que se encuentra en la trama.

Un escenario de desastre para una entidad de estas características, van desde daños físicos y lógicos como robos de información, desastres naturales, ciberataques, entre otros. En este capítulo, se tendrá como escenario de desastre un ciberataque, el cual puede ir desde un ataque DDoS, robo de información, accesos no autorizados hasta el daño de los datos almacenados en las bases de datos. Se listarán los detalles en la simulación del ataque.

El ataque, de forma general, será un exploit de vulnerabilidades en un ambiente controlado, de tal manera que produzca una indisponibilidad de servicios. Cabe destacar que lo realizado solo es una simulación para aplicar el plan de contingencia trazado.

El escenario de desastre será un ataque Smurf en los servicios del centro de cómputo principal. Una vez detectado el ataque y que los servicios hayan caído se cambiará a la contingencia para que los servicios estén disponibles nuevamente.

6.2 Detección de un ciberataque

La detección de un ciberataque es una tarea complicada para un usuario normal, por tal motivo, es necesario que el departamento de seguridad informática brinde pautas básicas, no solo en el cuidado del tratamiento de la información que administran en sus estaciones de trabajo, sino informar al personal sobre ciertas acciones potencialmente perjudiciales como son apertura de correos desconocidos, compartir archivos a través de memorias flash sin autorización, compartir claves de acceso de sus cuentas empresariales a desconocidos o terceros (proveedores de servicios). Cuando la estación del usuario ha sido infectada por algún código malicioso (típicamente virus) se debe capacitar al personal en la detección de bajo rendimiento en sus estaciones de trabajo (computadora lenta, navegación intermitente, archivos y accesos directos “borrados”, etc), e indicar que a la menor sospecha de infección deben informar al departamento de seguridad informática lo más pronto posible.

El departamento de seguridad informática puede realizar las siguientes revisiones de primera mano:

- Actividad de Disco Duro inusual.
- Archivos o directorios desconocidos.
- Procesos desconocidos o nombrados como procesos reales.
- Tráfico de red sospechoso, generalmente muy alto.
- Conexiones a una única Dirección IP.
- Alertas masivas del antivirus.

- Archivos sospechosos en carpetas temporales.
- Servicios instalados que no constan en el perfil autorizado.
- Contraseñas modificadas.

Las revisiones listadas son válidas para estaciones Windows y Unix (Linux), así como para servidores que poseas los sistemas operativos indicados. Los ciberataques muchas veces no son detectados hasta que es visible para el mundo, por ejemplo, el cambio de la página inicial de un website, mostrando un contenido erróneo o en otros casos no encontrándose disponible, ello aunque el servicio esté habilitado y funcionado en el servidor.

6.3 Comportamiento de los sistemas afectados

Los sistemas afectados por una intrusión o virus generalmente no presentan “síntomas” graves (salvo excepciones). Sin embargo, existe cierto comportamiento que cada usuario debe tener presente cuando se encuentre trabajando en su estación.

En el comportamiento de los servidores se observa el rendimiento y consumo de recursos, por ejemplo, en un servidor web se afectan los servicios de conexiones de usuarios para visualizar o descargar el website de la empresa o institución hasta que se consuman los recursos del equipo y genera una indisponibilidad del servicio web.

El comportamiento de los equipos de comunicación difiere en el consumo de recursos. Sin embargo, dependiendo de la configuración que posea en el momento del ciberataque, un atacante puede valerse de los protocolos de red soportados por el equipo y enmascarar su tráfico para evitar ser bloqueado por firewalls, routers o switches (capa 3). Una vez conectados se puede observar un aumento de tráfico en sus puertos y conexiones simultáneas hacia una sola IP externa, pudiendo bloquear los puertos y generar indisponibilidad de servicio, como se muestra en la figura 6.1:

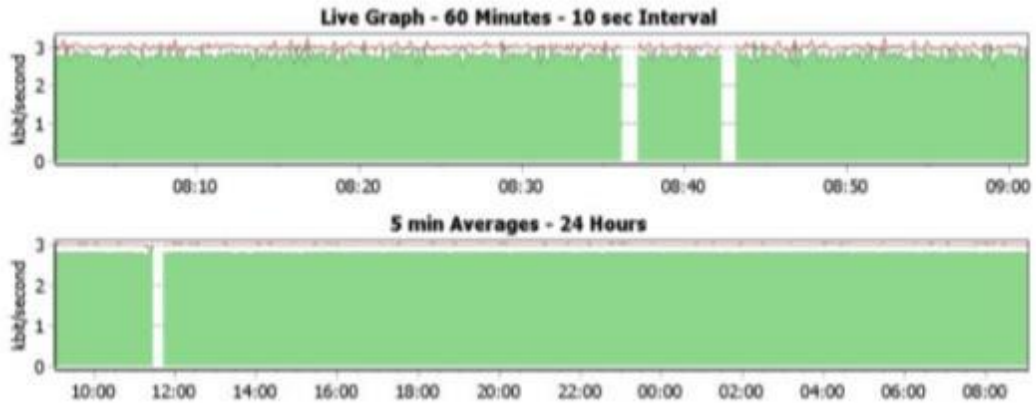


Figura 6.1 Saturación de enlace de datos

El comportamiento global del centro de datos se afecta a nivel lógico, es decir, sistemas de archivos, almacenamiento, nivel de procesamiento de solicitudes, saturación de ancho de banda, demoras en operaciones en bases de datos, inhabilitación de consolas de antivirus o envío masivo de alertas que produce colapsos en los equipos (servidores y estaciones de usuario como se muestra en la figura 6.2), de tal manera que la administración se torna imposible por el colapso de la unidad y en ocasiones un reinicio forzado es la única manera de ingresar nuevamente, aunque esta tarea no es recomendable porque el sistema puede quedar inservible y las bases de datos (si es el caso) pueden llegar a corromperse por el apagado abrupto.

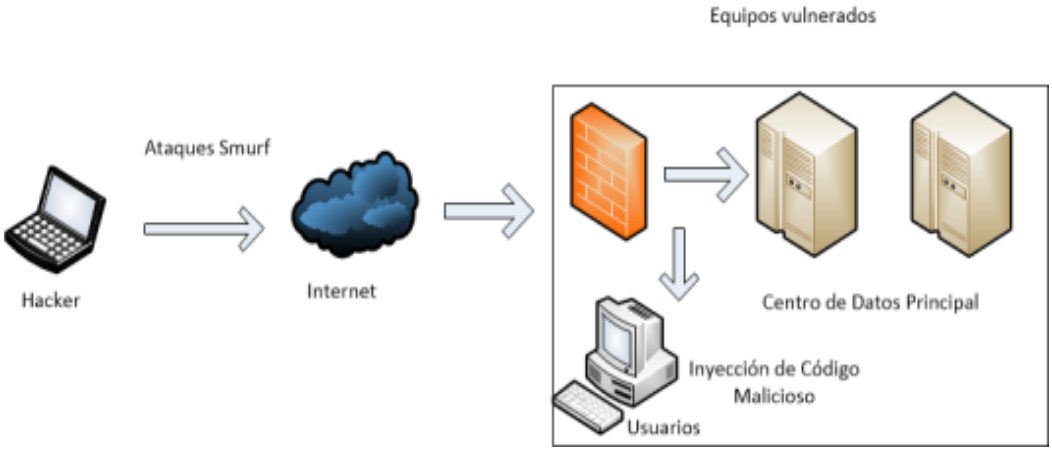


Figura 6.2 Equipos vulnerados por ataques

6.4 Gestión de recuperación

La gestión de recuperación es la aplicación de un plan de contingencia para la continuidad del negocio en caso de un ciberataque. El plan de contingencia a desarrollar primeramente se debe determinar el equipo operativo que hará frente al ataque, en este caso el área responsable es Seguridad Informática y el o la líder de Seguridad Informática debe garantizar lo siguiente:

- Proporcionar la disponibilidad de las copias de respaldo de los sistemas críticos y bases de datos en caso de requerirlo.
- Coordinar los enrutamientos de los enlaces contingentes hacia el CDV.
- Probar el sistema alterno en el CDV antes del paso a producción.
- Garantizar que el último respaldo de la base de datos, firewall, y demás, esté disponible en el CDV. De esto dependerá el tiempo fuera de línea.

Los pasos anteriores son pautas básicas que se deben tomar en cuenta para la puesta en producción del centro de datos en la nube (CDV). Se debe realizar simulacros al menos 2 veces al año para verificar tiempos de respuesta ante un posible ataque informático.

Se deben determinar los objetivos que ayuden a implementar procedimientos para responder ante ciberataques, pasar a una contingencia, mitigar la situación y regresar a operaciones normales en el centro de datos principal. Los objetivos son los siguientes:

- Identificar ciberataques según su tipo y determinar tiempos de respuesta.
- Desarrollar procedimiento ante ciberataques.
- Asegurar la legalidad de los procedimientos de contingencia.
- Definir responsables y sus funciones para aplicar el plan de contingencia.
- Establecer estrategia para regresar a operaciones normales (centro de datos principal).

El momento que se presente el ciberataque se deben ejecutar las acciones previamente planificadas de acuerdo a los objetivos listados anteriormente.

Las acciones se realizan en un orden, pero la ejecución se ejecuta en paralelo y coordinado ante un ataque informático (ciberataque) y la vuelta a la normalidad

una vez mitigado el evento. La planificación de las acciones a tomar son los siguientes:

Plan de Contingencia general

El plan de contingencia inicialmente puede contar con una serie de eventos potenciales que puedan comprometer la continuidad del negocio. Sin embargo, este documento solo se centrará en cualquier evento que sea catalogado como ciberataque y cuya consecuencia sea la indisponibilidad del servicio, esto es, comprometer el centro de datos principal y haya que utilizar el CDV. Los eventos potenciales que puedan ser catalogados como ciberataques son: Ataque DDoS, intrusiones ilegales, descarga de base de datos, filtro de información confidencial referente al negocio, infección de virus, instalación de software malicioso y ataques internos.

El plan de contingencia establece las acciones que se deben aplicar cuando uno de los eventos catalogados como ciberataques se presente, y su difusión se haga a través de los canales oficiales.

Los escenarios en que se presenten los eventos son cualquier momento del día o noche, por tal motivo se deben prever los siguientes escenarios:

- Durante el dia: 06:00-18:59
- Durante la noche: 19:00-00:00
- Durante la madrugada: 00:01-05:59

Los turnos correspondientes serán establecidos de acuerdo a los escenarios descritos, donde el área de Centro de Cómputo será un apoyo en horario no laboral, pero el área de Seguridad Informática seguirá siendo el responsable en cualquier momento del día, noche o madrugada.

Este plan deberá incluir la participación de todas las áreas involucradas de infraestructura y desarrollo, siempre liderados por Seguridad Informática, quien indicará paso a paso el cambio al CDV, pruebas de funcionamiento y puesta en producción del Data Center virtual.

Organización del personal involucrado

Establecer los equipos y asignar las funciones es una parte fundamental en el plan de contingencia para que cuando suceda algún evento, se ejecute la planificación de manera rápida y correcta, ya que el tiempo es primordial para que la baja de los servicios pueda ser vista como una intermitencia y no una indisponibilidad del servicio.

La premisa básica es la disponibilidad del servicio de forma permanente. Sin embargo, esto solo es ideal, ya que en la práctica se tienen intermitencias programadas (mantenimientos, revisiones, pasos a producción), y no programadas (fallo de equipos, cortes de energía) que de alguna forma afectan la disponibilidad del servicio.

El personal asignado de parte de infraestructura seria:

- Comunicaciones
- Centro de Cómputo
- Servidores
- Base de datos

El personal asignado de parte de desarrollo seria:

- Desarrollo de aplicaciones
- Control de calidad (software)

El líder será del área de Seguridad Informática. Se deber tener también un grupo de Relaciones Humanas para mantener informes al día acerca del evento al personal interno, externo, proveedores y clientes para tener una sola fuente de información. El líder de Seguridad informática es el único autorizado para generar informes oficiales hacia el grupo de Relaciones humanas.

Los grupos involucrados serán los siguientes:

Equipo de Seguridad Informática: Encargado de dirigir las acciones durante la contingencia y recuperación. Este grupo también es el encargado de coordinar los demás equipos o grupos; también se encarga de documentar el evento y

definir políticas y procedimientos a nivel de seguridad en infraestructura y desarrollo.

Equipo de Comunicaciones: Grupo encargado de realizar migraciones de los enlaces de datos en coordinación con los proveedores del servicio, actualización de reglas de firewall hacia el CDV y demás configuraciones que se necesiten en los equipos de su administración; luego de realizado los cambios en el CDV se deben realizar pruebas e informar al líder de Seguridad Informática la finalización de los cambios para que este autorice la puesta en producción del CDV.

Equipo de Centro de Cómputo: Grupo de operadores del Data Center principal, encargados del monitoreo del sistema y gestión de primer nivel sobre incidentes rutinarios y de impacto medio. Son los encargados de verificar el estado de los servicios y su funcionamiento tanto en producción como en contingencia. En condiciones de operaciones normales este grupo responde a la jefatura de infraestructura, gerencia tecnológica y gerencia general. Sin embargo, al momento operar con la contingencia solo responde al líder de Seguridad Informática y solo a él (ella) se le reportarán los eventos suscitados.

Equipo de Servidores: Grupo encargado de los servidores y sus sistemas operativos; son los responsables de administrar y gestionar los snapshot de todos los servidores y la configuración paralela en el CDV. Su función prioritaria en caso de emergencia es brindar el soporte necesario al área de Seguridad Informática en caso de ser necesario, una reconfiguración en el CDV.

Equipo de Base de Datos: Grupo encargado de las bases de datos de producción y desarrollo en su administración, gestión y aplicación de mejoras, así como del mantenimiento de las mismas. Durante el paso a Contingencia, serán los encargados de actualizar la información de las tablas a través de los respaldos; en este punto, tendrán el apoyo del equipo de Centro de Cómputo para proporcionar dichos respaldos. El tiempo de restauración es importante y de él dependerá el paso a producción de la contingencia.

Equipo de Desarrollo de Aplicaciones: Grupo encargado del desarrollo de aplicaciones propias de la empresa, tanto en materia de procesamiento de

datos, estadística de indicadores, información de volumen de ventas. También se encarga de proporcionar un ambiente para el usuario interno y de acuerdo a su área ayudar a realizar su trabajo de manera eficiente. Durante el paso a la contingencia este equipo será el encargado cargar en el CDV las últimas actualizaciones de sus aplicaciones y verificar su correcto funcionamiento.

Equipo de control de calidad: Grupo encargado de probar las nuevas versiones y aplicaciones de parches en las aplicaciones propias de la empresa, tanto para el procesamiento de información como aplicaciones para usuarios internos. Durante el paso a contingencia, este equipo se encargará verificar las últimas actualizaciones de las aplicaciones implementadas en el CDV por el equipo de desarrollo.

Procedimiento de repuesta

El procedimiento de respuesta, son los pasos a seguir cuando se dispara la alerta de un ciberataque. Para esto se debe tener un checklist con los contenidos del plan propuesto por el líder de Seguridad Informática, la aprobación de este procedimiento. Estará a cargo de Jefatura y Gerencia de Tecnología.

Los procedimientos incluyen los pasos antes, durante y después del ataque y son dependientes de la estrategia de recuperación. Agrupan las pruebas que se deban realizar estableciendo ventanas de ejecución ya sea de simulación, interrupción total o parcial ante un ciberataque, se puede ejecutar las pruebas en paralelo sin interrupción del servicio, emulando la modalidad de “balance de carga” pero ante una amenaza, ataque o baja de servicios se puede contaminar la contingencia.

Las pruebas son desarrolladas en la fase de mantenimiento y sirven para posteriores auditorias del sistema a ser ejecutadas.

Los procedimientos deben seguir una secuencia cronológica ante un evento de seguridad informática (ciberataque) y a la vez subdividido en fases y la activación de cada una desempeña una acción importante en el plan de contingencia:

- Fase de Alerta
- Fase de Transición
- Fase de Recuperación

Fase de Alerta: Incluye la detección de los primeros momentos del ataque y puede ir desde la afectación parcial como pérdida total del servicio catalogados como críticos.

Esta fase se subdivide en 3 partes:

- **Notificación:** En esta etapa se define quien deber ser informado en primera instancia ante un ciberataque y en caso de comprometer estaciones de trabajo, informar a los usuarios internos para la detención inmediata de labores y apagado de sus equipos. El líder de seguridad informática debe estar informado y a su vez, este informará a los equipos de las diferentes áreas tecnológicas para estar alertas en caso de paso a contingencia.
- **Evaluación:** En este punto, la situación se evalúa y valora inicialmente los daños con la mayor recopilación de información posible, los equipos involucrados en la aplicación del plan de contingencia están en espera a que se determine el estado de emergencia. Este paso no puede tomar mucho tiempo, ya que ante un ciberataque el tiempo es valioso para evitar daños irrecuperables en los datos e intrusiones más profundas que conlleven a robos de información y comprometan la integridad de la empresa.
- **Ejecución:** Cuando se ha declarado estado de emergencia, el líder de Seguridad Informática empieza con la aplicación del plan de contingencia movilizando a los equipos del área de tecnología (comunicaciones, servidores, base de datos, centro de cómputo, desarrollo y control de calidad) para que cada uno empiece las acciones ya establecidas para detener producción y migrar operaciones a contingencia (CDV).

Fase de Transición: Esta etapa del plan de contingencia es la fase previa de la migración del Centro de Datos principal hacia el CDV en el menor tiempo posible y se debe asegurar lo siguiente:

- Comunicaciones establecidas hacia el CDV.
- Información actualizada de la base de datos.
- Verificación de sistemas operativos en las máquinas virtuales.
- Actualización y verificación de versiones de aplicaciones propias de la empresa.
- Informar a usuarios internos y clientes la subida de los servicios, tanto en contingencia como de vuelta a producción.

La fase de transición, abarca los procedimientos definidos, respaldos de información relacionada al negocio de la empresa, documentación y manuales de los sistemas, asi como del plan de contingencia y las acciones ejecutadas por los equipos, siempre coordinados por el líder de Seguridad Informática.

Fase de Recuperación: Esta fase se la puede catalogar como “regresar a la normalidad”, cuando el ataque haya sido mitigado se debe realizar lo siguiente:

- **Reunión del equipo de contingencia:** Para coordinar el regreso de operaciones al centro de datos principal se debe decidir la estrategia, es decir, seguir un procedimiento para revertir los cambios, ya que la nueva información solo se encuentra en el CDV y se debe migrar esa información por los diferentes equipos, bajo la supervisión del líder de Seguridad Informática.
- **Evaluación de daños:** Cuando el ataque haya sido mitigado, se debe evaluar de manera inmediata la magnitud del ataque y los daños (si existen) producidos en el sistema; también se debe tomar en cuenta el tiempo necesario para la recuperación de equipos que presenten fallos.
- **Actividades prioritarias del plan de contingencia:** La aplicación del plan de contingencia en su real aplicación, comparado con la planificación del plan, habrá daños reales que deben ser evaluados y listados a ser realizados desde el punto de vista de las actividades prioritarias y estrategias aplicadas para con la empresa. La dedicación del equipo hacia tareas temporales en apoyo al personal de los sistemas afectados es un punto a ser evaluado.

- **Evaluación de resultados:** Este apartado sirve para evaluar objetivamente todas las actividades realizadas, una vez concluidas las acciones del plan de contingencia, si fueron realizadas correctamente, tiempo de respuesta, circunstancias, comportamiento del personal de apoyo y equipos involucrados en la aplicación del plan de contingencia. Esta evaluación da como resultado la “retroalimentación del plan de contingencia” y un “listado de minimización de riesgos posibles que pudieron ocasionar o dar apertura al ciberataque”.
- **Retroalimentación del plan de contingencia:** La evaluación de resultados debe optimizar el plan de acción original, mejorando acciones del equipo que tuvieron dificultad y reforzando acciones que resultaron positivas. El elemento a evaluar es el costo operativo y económico, si no se hubiera tenido un plan de contingencia ante ciberataques.

Se realizará un plan de contingencia aprobado por jefaturas y gerencia, así como también será revisado con todo el personal involucrado en las tareas del plan de contingencia, así como los procedimientos puestos en marcha para recuperación del negocio y la reanudación de operaciones en el centro de datos principal.

Por último, el contenido del plan es el resultado final de la ejecución del proyecto y su desarrollo. Debe estar debidamente aprobado y formalizado de forma minuciosa, para minimizar las decisiones improvisadas, en caso de aplicarlo.

La figura 6.3, muestra de forma resumida la interacción del líder de seguridad informática con los equipos de cada área de tecnología, lo que indica de forma clara la importancia de una comunicación oportuna y eficiente para la coordinación de cada una de la tareas que cada equipo debe realizar y a su vez retroalimentar al momento de realizar pruebas de ejecución del plan de contingencia para mejorar continuamente los procesos para que, cuando se presente una anomalía en el sistema de carácter sospechoso todos el personal domine las acciones que deben ejecutar en el tiempo correcto para minimizar el impacto de las operaciones normales de la empresa o institución pública.

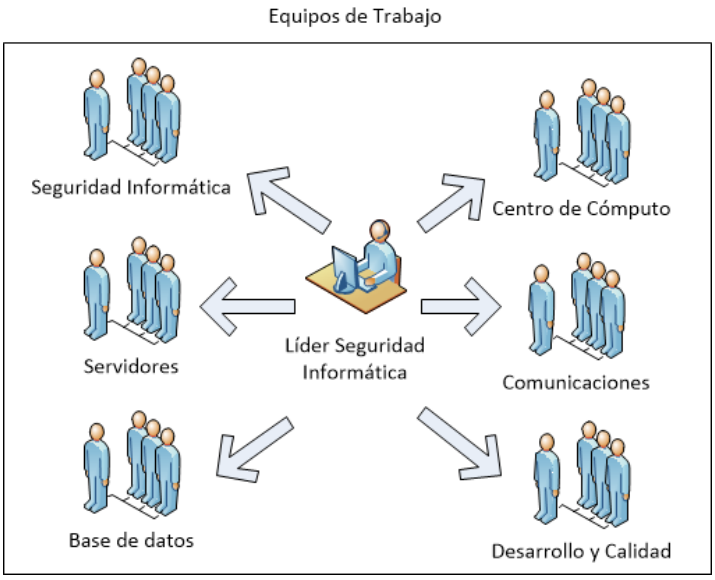


Figura 6.3 Líder de Seguridad Informática coordina a equipos de trabajo tecnológicos

Plan de contingencia ante ciberataques

El plan de contingencia general nos da una pauta de lo que se debe realizar y trazar los objetivos para minimizar en lo posible los daños del negocio de la empresa.

La empresa que se ha escogido para implementar un plan de contingencia es una empresa de ámbito financiero, con seguridades físicas y lógicas similares a un banco, pero con la particularidad que los valores monetarios físicos (dinero en efectivo) no son almacenados dentro de la empresa, sino que son depositados en una cuenta o varias cuentas en un banco que la empresa es cliente. Los valores lógicos (paypal, tarjetas de crédito, tarjetas de débito, etc) y sus comprobantes de pago son almacenados en la base de datos dentro de la empresa y su almacenamiento (disco duros y arreglo de los mismos) y es en este punto donde este elemento se vuelve crítico, ya que no solo almacena información sobre valores monetarios electrónicos, sino información de los clientes y la empresa garantiza la confidencialidad sobre las transacciones realizadas sobre su plataforma.

La empresa que hemos escogido se dedica a receptar pagos de todos los establecimientos a nivel nacional como:

Pagos de consumo a casas comerciales: DePrati, La Ganga, Artefacta, Creditos Economicos; Pycca, RM, Eta Fashion.

Pago de compra/venta por catálogo: Avon, Yanbal, Mi Angel

Pago de servicios básicos, televisión pagada e internet: Servicio de agua, luz y teléfono, televisión pagada e internet de todas las empresas a nivel nacional.

Pago de servicios públicos: Pago de matriculación Vehicular, formularios de impuestos (IVA, ICE), valores de municipios, RISE, liquidaciones del SENAE.

Pagos de tarjetas de crédito: Bancos y Cooperativas emisoras de tarjetas visa y mastercard, asi como American Express y Diners Club.

Pagos varios a proveedores: Esta categoría se creó con el fin de que PYMES o personal naturales que ofrezcan servicios profesionales puedan inscribirse y sus honorarios o facturas puedan ser canceladas en cualquier punto autorizado, los pagos receptados son en efectivo, cheque certificado, tarjeta de crédito, Paypal.

La empresa tiene su sede en la ciudad de Guayaquil, y su centro de datos principal se encuentra en los mismos predios. Existen pequeñas sucursales a nivel nacional ubicadas en sitios estratégicos como lo son las gasolineras; se ha escogido este tipo de establecimientos debido al gran flujo de personas que transitan en ellas. Las ciudades de Quito y Cuenca cuentan con oficinas con personal de talento humano, comercial, técnico y atención a clientes tanto en oficinas como en los puntos de pago.

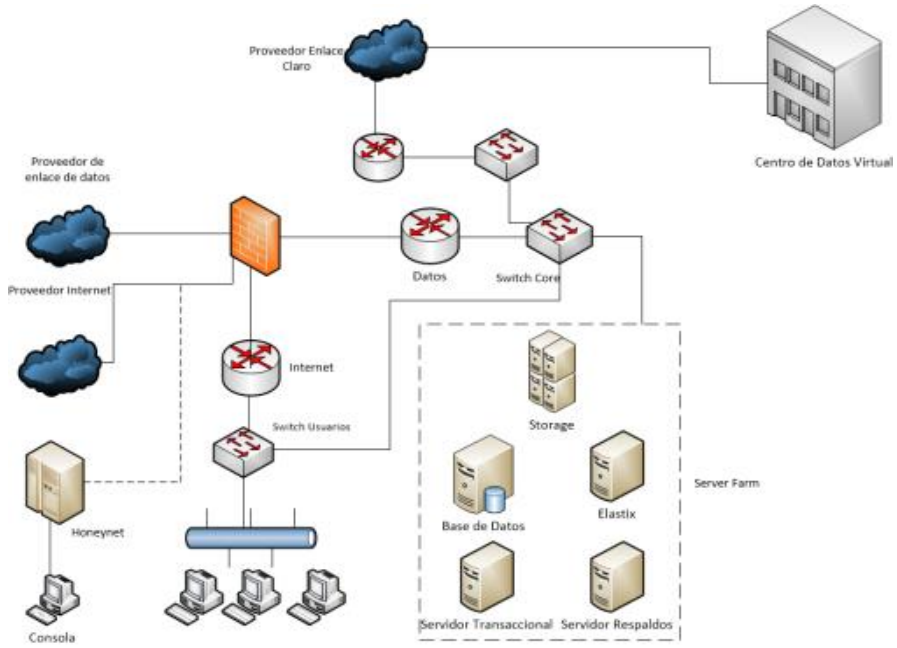


Figura 6.4 Diagrama de red básico de la empresa de Pagos electrónicos

Se ha realizado un análisis del negocio, la infraestructura informática, seguridades de valores lógicos, personal de sistemas, políticas de seguridad informática y responsables del área de infraestructura y desarrollo y se encontró lo siguiente:

- La política de seguridad debe actualizarse.
- Las contraseñas deben ser más fuertes.
- Control de acceso restrictivo al centro de cómputo.
- Area de Seguridad Informática debe ser creado.
- No existe de plan de contingencia en la empresa.

La gerencia general y de tecnología han decidido aplicar las normas de seguridad necesarias que se recomienden y han propuesto la creación de un plan de contingencia ante ciberataques, ya que han sufrido de filtración de información sensible de la base de datos de producción mediante programas de código malicioso aun teniendo firewall y antivirus instalados. Se pretende la capacitación del personal de Seguridad Informática y ajuste de los perfiles del área con la finalidad de que exista al menos 2 personas que se encarguen del

monitoreo de todo el sistema y revisión, aplicación y creación (según sea el caso) de manuales y políticas institucionales en materia de seguridad de la información.

Objetivos del plan de contingencia

Los objetivos del plan de contingencia establecen las metas a alcanzar para con la empresa y su continuidad de operaciones. Los objetivos son:

- Definir políticas de seguridad de la información en caso de ciberataque.
- Establecer procedimientos para área de tecnología y usuarios internos.
- Constituir y capacitar los equipos de tecnología a involucrarse en el plan de contingencia.
- Crear y socializar el procedimiento para la ejecución del plan de contingencia.

Los objetivos y los procedimientos, así como los manuales, deben ser elaborados en conjunto con las gerencias técnica y general para revisar propuestas y aprobarlas mediante reuniones semanales, quincenales o mensuales, según se decida en primera reunión.

La primera reunión del líder de Seguridad Informática con las gerencias, sirve para establecer la frecuencia de revisión de avances (reuniones), la conformación de los equipos de tecnología, asignación de roles para una potencial emergencia y a sus líderes la revisión del perfil necesario, en caso de no coincidir en al menos un 60%, se deberá capacitar en sus falencias; también se realiza un análisis del negocio (ya fue tratado en el apartado anterior), para exponer que se desea proteger, en este caso la información procesada y almacenada en el centro de datos, luego se procede a realizar un análisis de los riesgos y situaciones que sean consideradas como ciberataques, tanto internos como externos; aunque este análisis debe realizarse en primera instancia por el líder de Seguridad Informática, debe socializarse con la gerencia para establecer los parámetros que se necesiten en ese momento para tener un plan de contingencia, hablando desde el punto de vista económico (costo/beneficio) y deben exponerse las amenazas y vulnerabilidades del sistema.

Una vez realizada la primera reunión, se establecen los siguientes hitos:

- Establecer los equipos de tecnología involucrados en el desarrollo y aplicación del plan de contingencia y su respectiva asignación de roles.
- Trabajar con los equipos de tecnología para implementar el Data Center Virtual.
- Realizar al menos 2 pruebas al año para probar y mejorar el plan de contingencia.

Análisis de amenazas informáticas

Las amenazas y ataques posibles pueden sintetizarse en una tabla (ver tabla 17) con ataques intencionados o accidentales, pero ante un ciberataque se presume que todos los eventos son intencionados y establecer varios escenarios con su nivel de protección y cual sería una respuesta de acuerdo a la información recabada al inicio, estas serían actualizadas al momento de aplicar el plan de contingencia

Ataques o Amenazas	Posibilidad
Uso de software no autorizado	SI
Acceso no autorizado a información de la empresa	SI
Uso de software malicioso o fraudulento	NO
Robo de equipos informáticos	NO
Robo de información del negocio de la empresa	SI
Robo de fuentes de software propietario	SI
Descarga de software no autorizado	NO
Vigilancia de líneas de comunicación o enlaces de datos	NO
Abuso de privilegios de usuario	SI
Presencia de virus en la red interna	SI
Ataques mediante ingeniería social	SI
Ataques DDoS o Smurf	SI

Errores no accidentales	SI
Copias de información en medios magnéticos	NO
Errores en mantenimientos del sistema	NO
Corrupción de datos	SI

Tabla 17 Ataques o amenazas informáticas posibles

De acuerdo a la tabla 17, que muestra los ataques y sus posibilidades, se puede verificar que existen amenazas que pueden suceder y otras que no, ya que la empresa posee políticas de seguridad implementadas a nivel físico y lógico, pero que al momento no son suficientes para garantizar la continuidad del negocio.

Las vulnerabilidades se pueden identificar mediante posibles escenarios, y a partir de estos se identifican cuales pueden cumplirse con facilidad y cuáles no (ver tabla 18).

ESCENARIO	PROTECCION	RESPUESTA
Plan de recuperación carente o insuficiente	¿Existe plan de contingencia?	No, pero se está planificando
Fallos de energía eléctrica	¿Existe respaldo energético?	SI, UPS y generador para centro de datos
Personal técnico sin perfil requerido	¿Existen ingenieros inexpertos?	NO, el equipo técnico domina el sistema
Pérdida de información sensible de la empresa	¿Existen copias de seguridad de todo el sistema?	Parcialmente, se realiza en cintas magnéticas tipo LTO
Accesos no autorizados al centro de datos	¿Existe control del personal externo e interno?	SI, a través de accesos biométricos autorizados por el líder de seguridad informática
Privilegios de usuario inadecuados	¿Existen usuarios con privilegios no acordes a su perfil?	NO, los privilegios son aplicados de acuerdo a un perfil ya establecido

Robo de datos	¿Existen vulnerabilidades del personal o del sistema?	SI, la empresa ha sufrido filtración de información clasificada
Perdida de servicios por virus	¿Existe un plan de continuidad del negocio?	NO, se está realizando al momento
Uso de software de internet no autorizado	¿Existe control del software instalado?	Parcialmente, la revisión no es periódica

Tabla 18 Posibles escenarios de amenazas informáticas y nivel de protección

Como se puede apreciar, dentro de algunos escenarios comunes, las vulnerabilidades de la empresa son evidentes y deben ser considerados en el plan de seguridad y de contingencia, de tal forma que las amenazas sean minimizadas en el sistema.

Análisis de Impacto

Luego de manifestar las vulnerabilidades y las amenazas como consecuencia de estas vulnerabilidades, se debe definir el impacto que pueden producir estos eventos a la estabilidad del negocio; por tal motivo, se identificarán y analizar los procesos que pueden sufrir una amenaza y determinar su importancia para la empresa.

Unos formularios nos ayudarán a identificar estos procesos, su dependencia y los responsables de dichos procesos y su frecuencia, de esta forma, se puede tener una idea de las consecuencias de que interrupción de tal o cual proceso puede afectar a la normal operación del centro de datos y en extensión el negocio de la empresa. Los procesos como tal son:

- Webservice hacia los bancos
- Consolidación de información en línea
- Aplicación general para gestionar transacciones
- Generar facturas electrónicas
- Procesar información en base de datos

- Almacenar información, disponible para revisiones históricas
- Generación de indicadores gerenciales
- Revisión de transacciones para facturar a clientes (en caso de problemas)
- Procesos financieros internos de la empresa
- Mejoras tecnológicas en aplicativos y productos

Los procesos listados en la tabla 19, son los más importantes dentro de la empresa, ya que no solo procesan, almacenan la información y la transmiten hacia otras entidades, sino que es tratada internamente por las áreas de inteligencia de mercado y seguridad informática, los cuales realizan un análisis del negocio para establecer tiempos de respuesta y revisiones tecnológicas (respectivamente), uso de los productos y generar informes para gerencia y este a su vez, eleva los resultados a los accionistas de la empresa. Alguna interrupción en ellos significa pérdida de dinero, ya que por cada transacción que ingresa al sistema representa un margen de ganancia para la empresa y el mantenimiento del sistema.

Proceso	Área responsable	Descripción	Frecuencia*	Procesos Co-dependientes
Webservice hacia los bancos	Infraestructura y Desarrollo	Conexión a los bancos para gestionar los pagos electrónicos	Diaria	Consolidación de información en línea , Aplicación para receptar pagos de clientes
Consolidación de información en línea	Financiero	Comparar reportes enviados por las entidades y las generadas por la empresa	Diaria	Webservice hacia los bancos
Aplicación para receptar pagos de clientes	Desarrollo	Software para gestionar pagos de clientes	Diaria	Mejoras tecnológicas en aplicativos y productos
Generar facturas electrónicas	Infraestructura y Desarrollo	Envío de facturas hacia clientes de la	Diaria y Mensual	Consolidación de información en línea, Procesar información en base de datos

* La frecuencia se basa en experiencia del autor en administrar servicios electrónicos financieros.

		empresa y proveedores		
Procesar información en base de datos	Infraestructura	Administrar la información y enviarla a Seguridad informática e inteligencia de mercado	Semanal	Procesos financieros internos de la empresa
Almacenar información para revisión histórica	Infraestructura	Información siempre disponible para realizar comparativas mensuales, semestrales y anuales	Diaria	Procesar información en base de datos, Generación de indicadores gerenciales
Generación de indicadores gerenciales	Inteligencia de mercado	Reportes hacia gerencia para determinar	Mensual	Almacenar información para revisión histórica

* La frecuencia se basa en experiencia del autor en administrar servicios electrónicos financieros.

		cumplimiento de metas y estado de la empresa		
Revisión de transacciones para facturar a clientes o empresas (en caso de problemas)	Seguridad Informática y Desarrollo	Análisis de información contenida en transacciones para resolver conflictos con valores cobrados o depositados	A demanda	Procesar información en base de datos, Consolidación de información en línea
Procesos financieros internos de la empresa	Infraestructura y Desarrollo	Gestiona pagos a proveedores, cobro a empresas y pago de nómina de la empresa	Mensual	Almacenar información para revisión histórica, Consolidación de información en línea

* La frecuencia se basa en experiencia del autor en administrar servicios electrónicos financieros.

Mejoras tecnológicas en aplicativos y productos	Desarrollo	Agrega o quita diferentes opciones del software para realizar la atención al cliente de forma más eficiente	Mensual	Generación de indicadores gerenciales

Tabla 19 Cuadro de procesos propios de la empresa

* La frecuencia se basa en experiencia del autor en administrar servicios electrónicos financieros.

Se puede apreciar de la tabla 19, que existen procesos importantes que dependen de otros procesos para funcionar, tanto para generar información como para procesar resultados y generar estadísticas que, mediante una mejora continua ayudan a crecer a la empresa financieramente y comercialmente, siempre verificando sus productos, fortaleciendo alianzas estratégicas y sirviendo al cliente de forma eficiente, ya que la velocidad y el buen trato en la atención al cliente es algo fundamental en los negocios electrónicos en nuestros días.

El impacto de la paralización de alguno de los procesos implica perdidas monetarias, no solo por no realizar transacciones, sino porque se apuntala la credibilidad de la empresa y la confianza del cliente en la empresa.

Un escenario de ciberataque, es una denegación de servicio (DDoS), no solo por bloqueo de los puertos de comunicación, sino por la ejecución de código malicioso dentro del sistema afectando discos duros que contengan información del negocio de la empresa.

La tabla 20 presenta el impacto y su magnitud en la paralización de los servicios de la empresa, basados en el tiempo que tomaría el respaldo de una base de datos SQL típica, llevarla hacia la contingencia y restaurarla, siempre y cuando se cuente con un plan de contingencia:

Tipos de eventos	Magnitud del evento (tiempo)
Pérdida de ingresos	4 horas
Pérdida de beneficios	---
Impacto de flujo de caja	---
Incremento en gasto	4 horas
Impacto de operaciones	4 horas
Impacto Comercial	---
Impacto en calidad de servicio	4 horas
Impacto en Imagen	---
Desmoralización del personal	---

Tabla 20 Cuadro de eventos y su magnitud

Se puede notar, que se tiene un impacto controlado, siempre y cuando se cumplan las 4 horas desde la detección del ataque, cambio a la contingencia (CDV) y regreso al centro de datos principal; si este tiempo se excede, la pérdida de ingresos y el gasto, se incrementan pudiendo llevar a la empresa a una virtual banca rota. Por tal motivo es imperativo que el plan desarrollado se aplique al menos 2 veces por año para la familiarización con el mismo por el departamento de Tecnología.

Desarrollo del plan

El plan de continuidad del negocio (contingencia) ante ciberataques, se empieza a construir tomando en cuenta la estructura y composición de los equipos y sus acciones. Como ya se había comentado, en cada equipo habrá un líder y cuando se active el estado de emergencia estos responderán únicamente al líder de Seguridad Informática quien establecerá las directrices para la ejecución de procesos por parte de los equipos de tecnología.

La empresa es de tamaño medio con una meta de crecimiento de un 10% anual, por 5 años, debido a las afiliaciones de nuevos clientes que ingresan la red de pagos electrónicos, también se debe mantener a clientes ya existentes, por lo tanto, se ha decidido montar un CDV en lugar de la construcción de un Centro de Datos alterno propio, ya que con el crecimiento de clientes, es inevitable el crecimiento de equipos de procesamiento y almacenamiento de información, por lo tanto la construcción de un Centro de Datos alterno propio es una inversión que al momento la empresa no puede afrontar. Las actividades planificadas son:

Plan de emergencia: Se establecen una serie de calamidades o emergencias potenciales a nivel informático, como lo son los ciberataques; los cuales son todos los eventos que conlleve, robo de información mediante código malicioso, bloqueo del servicio a través de los equipos de comunicaciones de frontera, daño de equipos y sistemas operativos ejecutados por virus; se han mencionado las consecuencias de los ataques, sus causas más comunes y populares en nuestros días, es la ingeniería social en un correo electrónico, ya que valiéndose de la ingenuidad de los usuarios, envían cadenas o ejecutan archivos adjuntos

que, sin conocerlo, permiten la entrada a código malicioso. Se establecerán espacios de contingencia en todos los horarios, mañana, tarde o noche en días normales o feriados, el personal de tecnología siempre existirá una persona de StandBy para atender las posibles emergencias, ya sea remotamente o presencial, así como una lista de contactos (escalamiento) para solicitar apoyo o autorizaciones de parte de gerencia o el líder de Seguridad Informática.

Organización de equipos y sus tareas: La organización de los equipos tecnológicos, como ya se ha comentado, estará a cargo del equipo de Seguridad Informática, ya que, ante un ataque, este grupo realizará las acciones para mitigarlo, si toma mucho tiempo, se informa a gerencia y este decidirá si se declara la empresa en emergencia o no. En caso de que se declare en emergencia, se activan los protocolos de seguridad ya establecidos y solo en esta etapa los equipos de tecnología empiezan su accionar de acuerdo a las directrices del líder de Seguridad Informática, se pueden mencionar de forma general las acciones que debe realizar cada equipo:

Equipo de Seguridad Informática

- Detectar ataques en el sistema.
- Establecer el impacto de la amenaza.
- Informar a Gerencia los eventos críticos.
- Coordinar con los líderes de los demás equipos la aplicación del plan de contingencia.

Equipo de Comunicaciones

- Bloqueo del perímetro interno y externo.
- Coordinar con los proveedores de enlaces los cambios de ruta del tráfico externo e interno hacia el CDV.
- Activar honeynet en perímetro externo para evitar propagación de la amenaza.
- Informar al líder de Seguridad Informática cuando el honeynet se encuentre activado para su monitoreo, revisión y determinar plan para mitigar la amenaza.

- Actualizar reglas del firewall en el CDV y configuraciones de switch y router (en caso de ser necesario).

Equipo de Centro de Computo

- Monitorear el sistema y verificar funcionamiento de los servicios.
- Informar sobre novedades durante y después del ataque al líder de Seguridad Informática.
- Verificar conexiones hacia el CDV.
- Tener disponible los últimos respaldos de la base de datos de producción y del sistema en general.
- Verificar disponibilidad de servicios internos y externos cuando haya terminado el cambio.

Equipo de Servidores

- Bajar servicios red del sistema operativo y aplicaciones.
- Aislar los servidores de la red interna para verificación posterior, si un servidor está comprometido, apagarlo.
- Verificar y aplicar respaldos (si fuera necesario) en servidores del CDV con el apoyo del equipo de Centro de Computo.
- Verificar actualizaciones en servidores del CDV.
- Verificar procesos en servidores del CDV.
- Actualizar almacenamiento de datos en CDV (en caso de ser necesario).

Equipo de base de datos

- Cerrar las conexiones a la base de datos de producción.
- Bajar servicios y desmontar la base de datos.
- Verificar almacenamiento de la base de datos no crezca en espacio (en caso de que la base haya sido comprometida).
- Revisar los servicios y procesos de base de datos en el CDV.
- Restaurar la base de datos en el CDV (en caso de ser necesario) con el apoyo del equipo de Centro de Computo.
- Verificar los servicios y procesos de la base de datos en el CDV.

Equipo de Desarrollo de aplicaciones

- Verificar aplicaciones en el CDV y actualizarlas (si fuera necesario) con la última versión estable.
- Realizar pruebas de compatibilidad y funcionamiento en el CDV.
- Replicar configuraciones en las instalaciones del CDV para continuar operaciones desde la contingencia (remoto).

Equipo de Control de Calidad

- Verificar los cambios aplicados por el equipo de desarrollo en el CDV y certificar su óptimo funcionamiento.
- Controlar las versiones instaladas en el CDV, cumplan con las solicitudes o requerimientos ya implementados.
- Certificar las pruebas de funcionamiento de las aplicaciones del CDV.

Los equipos tecnológicos solo se encargan del paso del sistema desde el centro de datos principal hacia el centro de datos virtual; pero también es necesario mencionar equipos de otras áreas que de una u otra forma se ven involucrados en la aplicación del plan de contingencia, como son:

Equipo de recuperación: Este equipo es el equipo de tecnología, ya que ejecutan el plan de contingencia y también el proceso de vuelta a la normalidad, incluye un equipo de soporte técnico (usuarios internos), Equipo de Relaciones Públicas y Equipo de las unidades de negocio. Esta última, se conforma por cada gerente de área, quien se encargará de verificar el correcto funcionamiento de su área (PC, red, aplicaciones internas, etc.) y a su vez los replica al líder de Seguridad Informática y con el apoyo del equipo de soporte técnico, se verificarán los incidentes que presenten equipos de usuarios internos.

Equipo de Soporte Técnico: Este equipo será el encargado de verificar los equipos de trabajo de los usuarios internos, detectando si alguno se encuentra comprometido con algún código malicioso (se revisan los comportamientos de los equipos), si alguno se encuentra infectado se procede a aislarlo e inmediatamente se indica a los usuarios a apagar sus estaciones para evitar la propagación de la amenaza.

Equipo de Relaciones Públicas: Este equipo normalmente tiene la tarea de Community Manager, es decir manejar las redes sociales de la empresa, gestionar y dirigir requerimientos a las áreas respectivas. En caso de emergencia, ellos son los responsables de informar a los clientes y público en general mediante boletines oficiales los problemas que tiene la empresa y los trabajos que se realicen para su solución inmediata, este equipo es el único autorizado por gerencia y Seguridad Informática para emitir comentarios sobre el estado de la empresa sin menoscabar la confianza del público en el tratamiento de sus valores financieros.

Equipo de Unidades del Negocio: Este equipo se encuentra conformado por los líderes de las áreas no técnicas (administrativo, financiero, operaciones, servicio al cliente, etc) para definir la estrategia a seguir una vez que la contingencia haya sido puesta en producción y cuando se haya vuelto a operar con el centro de datos principal. Ellos necesitarán el “input” desde tecnología del estado del sistema para establecer tiempos de respuesta para trabajar con los procesos detenidos en sus respectivas áreas y afrontarlas de forma eficiente con sus equipos.

Procedimiento de respuesta

El procedimiento de respuesta, consta de 3 fases que, de forma general, se pueden explicar la aplicación del plan de contingencia.

Fase de alerta: La fase de alerta puede ser informado por cualquier usuario interno, ya sea porque su equipo esta con un comportamiento anormal o algún detalle que haya notado al realizar sus labores diarias; en este caso el líder de Seguridad Informática, a través del área de soporte técnico, debe evaluar el evento y si el mismo se replica en otros equipos. Se revisa el sistema para detectar posibles infecciones o intrusiones. De esta fase dependerá el impacto que el ciberataque o amenaza tenga sobre el negocio y también la ejecución del plan de contingencia.

Fase de Transición: La fase de transición abarca el paso de operación desde el centro de datos principal hacia el centro de datos virtual (contingencia) para de esta manera declarar el estado de emergencia en la empresa y los equipos

técnico y no técnicos ejecuten las tareas asignadas de forma independiente, siempre bajo la coordinación del líder de Seguridad Informática, de tal forma que las operaciones en el Centro de Datos Vritual puedan estar en línea en el menor tiempo posible con la información actualizada o al menos un desfase de un dia.

Fase de Recuperación: La fase de recuperación, incluye las acciones para la puesta en producción del Centro de Datos Virtual con la carga de información de las bases de datos, sistemas operativos y aplicaciones internas y externas, y también las pruebas de funcionamiento de todo el sistema por parte de los diferentes equipos tecnológicos. En esta fase también se implican a los equipos no técnicos para que apliquen sus estrategias propias y afronten los problemas generados por la interrupción de operaciones de forma eficiente y las notificaciones correspondientes a clientes y usuarios en general.

Fase de Vuelta a la normalidad

Una vez ocurrido el evento habiendo recuperado el sistema a través del Centro de Datos Virtual, es necesario realizar algunos pasos para regresar a operaciones normales una vez superado el incidente.

Realizar reuniones: Se debe planificar la vuelta a operaciones normales una vez que la amenaza se encuentre controlada y los sistemas hayan sido restaurados (si fuera necesario), garantizando su funcionamiento.

Evaluación de daños: Se detallan los daños que se han producidos por el ciberataque, vulnerabilidades en las comunicaciones, especialmente los firewalls, posibles daños en la base de datos (si hubiere), y en general se realiza una evaluación al sistema para determinar si se han sufrido daños que comprometan su integridad y necesiten reparación física o lógica para regresar a operaciones en el Centro de Datos Principal.

Priorizar y ejecutar actividades: Las actividades que se deben priorizar son las de mitigar la amenaza, una vez realizada, se debe reponer el sistema, por lo tanto, los equipos del área de tecnología realizaran las actividades para restaurar lo que tenga algún fallo lógico o físico, contacto con proveedores (si fuera el caso) para soporte especializado, reestructuración de reglas de acceso

al firewall y revocación temporal de todos los privilegios de usuario. Las comunicaciones son vitales en nuestros días, por lo tanto, los trabajos en esta área son críticas para la empresa y deben realizarse las pruebas necesarias antes de garantizar que las operaciones no vuelvan a sufrir interrupciones por el mismo motivo, durante la emergencia los líderes de cada área técnica responderán e informarán avances de su trabajo de restauración al líder de Seguridad Informática.

Evaluación de resultados: Los resultados se evalúan de manera objetiva y se esperan recomendaciones.

Feedback: El feedback (retroalimentación), es la información que recabamos con la experiencia del ciberataque y podemos obtener mejores resultados para ocasiones similares. Se analizan los problemas, contratiempos y se ajustan los procesos de recuperación.

Dependiendo de la seriedad del ciberataque, la vuelta a la normalidad de operaciones, puede tomar unas horas hasta varios días; lo importante es que el servicio hacia los clientes no se detenga y el trabajo de los usuarios internos de la empresa no se vean afectados en mayor medida; a partir de aquí, se genera otro plan, mejorado, revisado y aprobado, el cual se revisa con todos los equipos técnicos y no técnicos, tomando nota de los puntos de vista y experiencias durante el proceso de recuperación del sistema mediante un CDV.

6.5 APLICACIÓN DEL PLAN DE CONTINGENCIA

El plan de contingencia, una vez que ha sido planificado, podemos realizar una simulación sobre la aplicación del plan cuando un ciberataque ocurre, para esto primeramente notaremos los antecedentes, el negocio de la empresa y sus debilidades si se presenta una amenaza, como ya hemos indicado estos puntos en los anteriores subcapítulos del presente capitulo, solo realizaremos un resumen de los mismos para tener una mejor visión acerca del plan de contingencia ante ciberataques.

El ciberataque no solo se realiza en línea y mediante hackers, también es considerado como tal, la inyección de código malicioso (virus, troyanos),

mediante los cuales se aprovechan de sistemas operativos vulnerables para descarga de información, intrusiones forzadas (no autorizadas), robo de información confidencial de la empresa (espionaje industrial), convertir equipos informáticos en zombies y ser parte de Botnets (redes que usan otros equipos para lanzar ciberataques).

La empresa de pagos electrónicos, se constituyó como una competencia hacia las redes ya existentes en el país, como por ejemplo Red Activa (Western Union) y Servipagos (Produbanco), debido a la gran afluencia de clientes que se acercan a estos establecimientos para realizar el pago de servicios básicos, televisión pagada, servicio de internet, ventas por catálogo, pero también introdujo la recepción de pago a través de tarjetas de crédito y Paypal, así como la opción de registrar a profesionales y empresas (sin importar su tipo de negocio), para que sus clientes puedan realizar sus pagos sin tener que desplazarse hasta los banco u oficinas. Como ubicación estratégica se eligieron gasolineras, ya que en los últimos años el comercio ha crecido en estos establecimientos, como Terpel, Primax, PDV y Petrocomercial, dentro de sus tiendas.

La gerencia general, con el apoyo de Tecnología, habría acordado que se realizara una auditoria del sistema en cuestión para verificar el estado del mismo, identificando las posibles vulnerabilidades y establecer políticas de seguridad actualizadas de acuerdo con la realidad de la empresa y capacitación del personal interno para la correcta aplicación de dichas políticas. La auditoría habría obtenido el siguiente resultado:

- Políticas de seguridad aplicadas parcialmente, se necesita actualizarlas para implementar los cambios.
- No existe personal responsable para realizar solicitud de privilegios a usuarios, soporte técnico lo realiza bajo demanda y sin autorización escrita, solo verbal.
- Acceso a servidores (dominio, correo) lo realiza soporte técnico con privilegios de administrador.

- Plan de contingencia solo existe en caso de desastre físico, pero no se ha implementado. Los ciberataques no se han considerado, aunque ya han sufrido varios problemas por intrusiones no autorizadas y han estado fuera de línea entre 1 y 3 días, generando pérdidas a la empresa y está peligrando la renovación del acuerdo comercial con un cliente.
- Área de Seguridad Informática no existe como tal. Las tareas que debería realizar este departamento están delegadas entre el departamento de tecnología.
- Acceso a Internet es sin restricciones, incluso en el área de Centro de Cómputo.
- Los sistemas operativos de los servidores se encuentran parchados parcialmente o desactualizados y el antivirus no se encuentra en todos los equipos informáticos.

Los puntos antes mencionados, el más importante es la creación del área de seguridad informática, ya esta área se encargará de establecer las directrices para arreglar las vulnerabilidades que la empresa tiene y han sido documentadas en el informe de auditoría.

La aplicación del plan de contingencia se enfocará ante ciberataques, estableciendo un hipotético escenario de indisponibilidad de servicio, seguido con la inyección de código malicioso a través de una estación de trabajo ejecutado desde el buzón de correo de un usuario interno.

Se establece el escenario:

La empresa de pagos electrónicos se encuentra realizando los ajustes en materia de seguridad a nivel tecnológico con un avance del 90%, el cual es un valor arbitrario porque solo estamos estableciendo el escenario, esto incluye la terminación del plan de contingencia ante ciberataques y la contratación del Centro de Datos Virtual (CDV) con la empresa CLARO, en su división CLOUD (CLARO CLOUD), configuraciones de equipos, establecimiento de enlaces de datos dedicados desde el centro de datos principal hacia el CDV a través de una red independiente. Se tiene planificado realizar una prueba de funcionamiento simulando una amenaza, en un plazo de 30 días, cuando se haya terminado el

proyecto de seguridad informática y capacitación al personal de la empresa con las nuevas políticas de seguridad en el tratamiento de la información, al momento solo Tecnología conoce estos cambios.

La empresa ha sufrido un evento de ciberataques en su sistema en la modalidad de inyección de código malicioso, desde el equipo de trabajo del operador de Centro de Cómputo, la investigación realizada en esa época, por soporte técnico, concluye que la causa de infección fue a través de un correo (con archivo adjunto) que envió un proveedor de servicios aparentemente solicitando información acerca de las instalaciones físicas para realizar el paso de una fibra óptica y mejorar las comunicaciones. El código malicioso ejecutó un archivo .bat y desde la estación de trabajo del operador realizó la descarga de información sobre los productos nuevos y existentes ofrecidos por la empresa, así como parte de la cartera de clientes afiliados al sistema de pagos electrónicos; esta información la envía a través de una conexión ftp a una IP pública registrada a nombre de la empresa rival que también ofrece los servicios de pago. Mediante demandas y acuerdos de confidencialidad se pudo lanzar los productos sin perjuicio económico, y se pudo limpiar el sistema del virus.

La gerencia, temiendo un ataque similar o peor aún, quedando sin servicio optó por realizar el proyecto de seguridad informática. Como se comentó anteriormente, se planificó las pruebas de funcionamiento del plan de contingencia ante ciberataques en un lapso de 30 dias. Sin embargo, se adelantará la aplicación debido a los siguientes eventos:

- El miércoles a las 11:30, el equipo de seguridad informática detecta una serie de intentos de accesos mediante fuerza bruta al firewall, y es contenido cerrando el puerto de conexión.
- Luego a las 11:45, se realiza un ataque DDoS, tipo SMURF, haciendo que el firewall se ralentice y empiece a rechazar conexiones de los clientes, Seguridad Informática lo detecta, informa a gerencia e inmediatamente se establece el estado de emergencia.

- A las 12:00, un usuario reporta fallos en su estación de trabajo a soporte técnico, y se detecta la presencia de un virus por el siguiente comportamiento **[Anexo5]**:
- Consumo de disco duro al máximo, equipo se encuentra demasiado lento.
- Trafico de red elevado (más del 50%) visualizado en su tarjeta de red.
- Sistema operativo inestable debido al consumo de recursos.
- Procesos desconocidos se encuentran con nombres propios del sistema operativo.

El líder de soporte técnico indica a Seguridad informática que el antivirus fue deshabilitado y no detectó el virus. Se procede a aislar el equipo de la red.

El líder de seguridad informática informa que se aplicará el plan de contingencia ante ciberataques. Será implementado y los equipos tecnológicos se centran en las tareas ya informadas a través de la documentación del plan ya mencionado.

Desarrollo del plan de contingencia

1) Cuando la amenaza es detectada, el líder de seguridad informática informa a gerencia y se establece el estado de emergencia, durante este lapso, la máxima autoridad es el líder de seguridad informática.
2) El equipo de comunicaciones cierra las conexiones en los equipos de comunicación, y procede a activar el “Honeynet”. Coordina con proveedores de enlace de datos los cambios de ruta hacia el CDV y que permanezcan en standby para habilitarlos.
3) El líder de seguridad informática informa a los propietarios de los enlaces y servicios externos con los cuales se tienen convenio (banred, bancos, etc.), sobre el cambio a la solución de contingencia.
4) El equipo de base de datos cierra las conexiones en la base de producción, detiene los servicios y procesos; empieza a generar una copia de seguridad de la base de datos de modo incremental, para que sea subida hacia el CDV.
5) El equipo de servidores detiene los servicios de red de los equipos de producción ubicados en el centro de datos.

6) El equipo de Centro de Cómputo verifica los servicios tanto en el centro de datos principal como en el CDV.
7) El equipo de soporte técnico indica a los usuarios apagar inmediatamente sus estaciones de trabajo para evitar la propagación de la amenaza.
8) El equipo de Relaciones Publicas informa mediante un boletín la intermitencia que se tiene en el sistema.
9) Los equipos de comunicaciones y servidores empiezan a subir las actualizaciones en el CDV de los equipos que lo requieran. Firewalls y switches se deben actualizar en sus reglas y permisos, ya que estos parámetros cambian constantemente.
10) El equipo de base de datos empieza la subida y restauración de la base de producción ubicada en el CDV, esta tarea tarda en completarse alrededor de 2 horas y media, desde la generación del respaldo hasta su restauración.
11) El equipo de desarrollo actualiza las aplicaciones a sus últimas versiones cuando el equipo de servidores confirme que ha terminado las tareas en el CDV y en conjunto del equipo de Control de Calidad se verifica y certifica el correcto despliegue de las aplicaciones y su funcionamiento con las opciones y cambios implementados.
12) Cuando el área de base de datos informa que ha terminado la restauración de la base de datos en el CDV, se realizan las pruebas de transacción en el sistema a través de los equipos de prueba de la empresa.
13) Se indica a los proveedores de los enlaces que habiliten los enlaces hacia el CDV, poniendo de esta forma en línea el Centro de Datos Virtual y restaurando las operaciones con nuestra contingencia.

La puesta en línea de la contingencia demoró alrededor de 3 horas, debido a la limitante del tiempo de generación de respaldo de la base de datos, su copia hacia el CDV y la posterior restauración en la base de datos replica (en el CDV).

La amenaza fue contenida a las 18:15 del mismo día. Se concluyó que el ataque fue originado desde una IP ubicada en Alemania, como se muestra en la figura

6.5. Se realizó el bloqueo de dicha dirección en los equipos de frontera y se envió una solicitud al proveedor de internet para que realice la misma acción en los equipos con los cuales se brinda el servicio. La incorporación del “Honeynet” ayudó a engañar y mitigar la amenaza, ya que el “honeynet” actúa como una red paralela con las vulnerabilidades conocidas y el código malicioso siempre buscará el camino más fácil para ejecutarse.

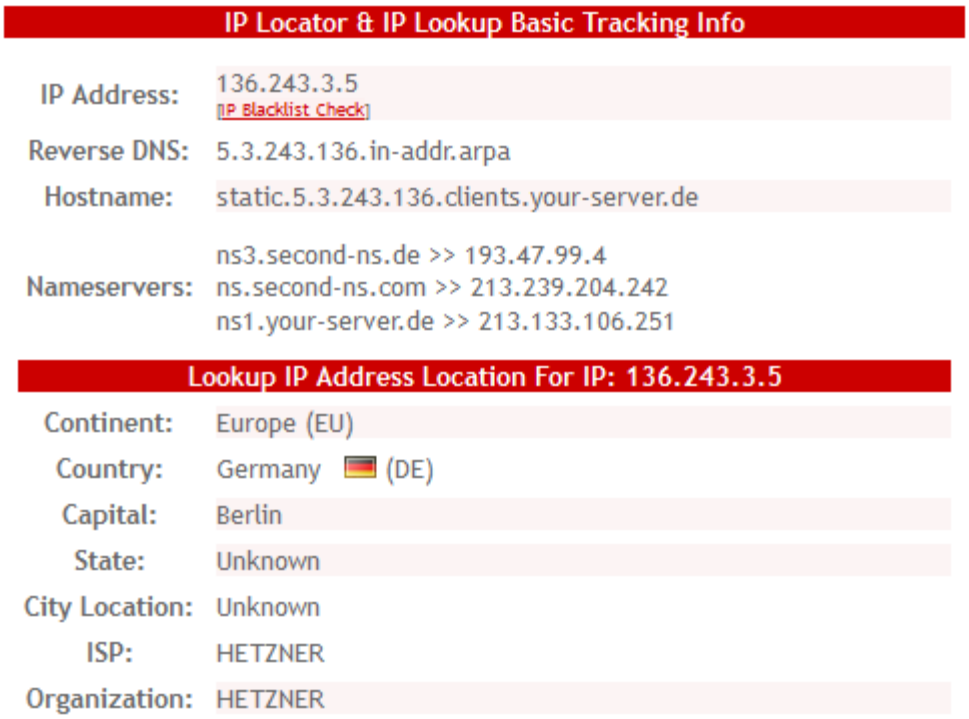


Figura 6.5 Localizacion de IP origen del ataque

El ataque SMURF fue repelido con éxito, no solo por el bloqueo de IP, sino deshabilitando ping y echo en los firewalls, switches y demás equipos que tengan salida a Internet y reconfigurándolos para estos fines. Si existiera daño en el equipo se aplicará la garantía adquirida al momento de la compra.

El virus que fue detectado en las estaciones de trabajo fue contenido cuando se había extendido a 8 estaciones, debido a la demora de los usuarios en apagar los equipos y el equipo de soporte no centró su atención a usuarios de atención al cliente. Se aplicó un antivirus portátil y herramientas de desinfección avanzadas.

Regreso a operaciones normales

Las operaciones ahora se encuentran en el Centro de Datos Virtual (CDV). La amenaza ha sido contenida y se debe regresar a operaciones normales, pero no podemos arriesgarnos de tener una nueva interrupción del sistema en horas de altas transacciones, por lo tanto se debe seguir los pasos anteriormente listados para la “Vuelta a la normalidad”. Por lo tanto se realiza lo siguiente:

- Los líderes de las áreas técnicas y no técnicas se reúnen para planear la estrategia a aplicar para regresar las operaciones a la normalidad, incluso se definen horarios de bajo volumen de transacciones para minimizar el impacto de la indisponibilidad del servicio. Así mismo, se realizan reuniones al interno de cada área para definir las acciones que se deben tomar por problemas operativos que surjan por parte de los clientes en alguna transacción que hayan realizado en el momento de la indisponibilidad.
- Durante las reuniones se exponen los daños sufridos por cada área, sea físico o lógico, para de esta manera evaluarlos y a través de la experiencia determinar los correctivos para solventarlos y convertir esa debilidad en una oportunidad para mejorar, es decir, planificar las acciones a realizarse para que, ante un nuevo evento, los daños sean menores o nulos.
- La vuelta a la normalidad es tan importante como aplicar la contingencia misma, por tal motivo, se deben priorizar las actividades que conlleven esta fase de reverso al Centro de Datos Principal por parte de los equipos técnicos; sus funciones quedan relegadas a segundo plano hasta el término del estado de emergencia, toda la atención y energías deben estar focalizadas en el paso del Centro de Datos Virtual hacia el Principal. En esta fase también se coordina con proveedores la aplicación de garantía de los equipos (si fuera necesario).
- Una vez que se han definido las estrategias para regresar a la normalidad en operaciones y se han priorizado las acciones de cada equipo, se ejecutan las tareas de reverso de la contingencia y se

preparan los equipos a ser reconfigurados como la base de datos, cuya información nueva debe residir en el centro de cómputo principal y se realizará ejecutando un respaldo en la base del CDV y restaurándola en la base del CDP (centro de datos principal). Como este es el punto que toma más tiempo, se decidió realizar el reverso de la contingencia en el horario de 01:00 a 04:00.

- Cuando se haya regresado a operaciones normales se debe realizar una evaluación de los resultados.
- La experiencia y las pruebas que se realicen al plan de contingencia se podrá obtener mejores resultados aplicables en eventos futuros. Se analizan las dificultades encontradas tanto en el sistema como en los equipos al momento de aplicar la planificación y el paso a contingencia será más preciso.
- La vuelta a la normalidad dependerá de los daños que se hayan sufrido en el sistema principal, puede ser unas horas o varios días hasta tener todos los equipos verificados y luego de las pruebas de funcionamiento pertinentes luego del evento.

6.6 Evaluación de la estrategia aplicada

Se ha planteado una situación de emergencia que en el ámbito de ciberataques es común, ya que se trató de un ataque DDoS y una infección por virus. Se ha propuesto una institución financiera como ejemplo, ya que poseen negocios sensibles a cualquier interrupción del sistema, enlaces de datos, etc. No es más importante que la paralización de operaciones en una fábrica, es más, se debe tratar con la misma importancia a las empresas sin importar el negocio que posean, ya que las interrupciones o indisponibilidad de servicio tiene como consecuencia perdidas de dinero que dependiendo de la gravedad del incidente, pueden llegar a ser irrecuperables así como también puede significar la desaparición de la misma. La estrategia aplicada, una vez detectada y evaluada la amenaza, consiste básicamente en lo siguiente:

- Establecer el estado de emergencia en la empresa.

- Informar a los líderes de cada área sobre la amenaza y autorizar la ejecución de las tareas ya establecidas para la aplicación del plan de contingencia.
- Informar a clientes la intermitencia de los servicios a través de un boletín, enviado por el equipo de Relaciones Públicas.
- Equipos no técnicos tomaran decisiones acerca del enfrentamiento del problema, sus estrategias para mitigar el impacto en los clientes y acciones luego del reverso de la contingencia.
- Cuando la contingencia se encuentre en producción, los líderes de las áreas se reúnen para decidir la estrategia y horarios de reverso de contingencia (regreso a operar con el Centro de Datos Principal).

Estas acciones podemos garantizar el levantamiento del centro de datos de contingencia en cuestión de horas, siempre y cuando, desde el área de tecnología garanticen las operaciones y el correcto funcionamiento del Centro de Datos de Contingencia, eso dependerá del tipo de tecnología y equipos que la empresa esté utilizando, por tal motivo, esos parámetros de configuraciones técnicas no son consideradas en el presente documento al ser altamente volátiles.

La evaluación del plan de contingencia puede darse desde diferentes puntos de vista, por ejemplo, tiempo de ejecución del plan (eficiente o eficaz), conocimiento del plan y tareas específicas por parte del equipo de tecnología, confianza del líder de Seguridad Informática por parte de su equipo técnico.

El plan de contingencia se evaluaría bajo los siguientes parámetros:

- Dificultades encontradas por el equipo técnico.
- Porcentaje de error que se puede asumir por problemas externos.
- Motivación de los equipos técnicos y no técnicos para enfrentar el evento.
- Conocimiento del plan de contingencia ante ciberataques.
- Procedimientos detallados y documentados

Dificultades encontradas por el equipo técnico

Las dificultades que se pueden encontrar van desde la indisponibilidad de la estación de trabajo hasta la ausencia del responsable o líder de equipo por enfermedad, vacaciones, o algún evento que obligue su estadía fuera de oficina, por tal motivo, debe haber una persona de Backup que solvente las ausencias e incluso se pueda coordinar desde su estación de trabajo. En este parámetro se elaboraría un checklist de los eventos posibles, añadiendo o quitando según sea el caso. Se asigna un 20% para evaluar este parámetro.

Porcentaje de error que se puede asumir por problemas externos

El porcentaje de error asumido por problemas externos, significa, que tanto porciento la empresa puede soportar desde la presencia del ataque hasta empezar la aplicación del plan de contingencia, esto puede ser debido por problemas en los enlaces de datos o con la plataforma del CDV o algún equipo que dependa de la intervención de personal ajeno a la empresa (proveedor). Se elaboraría un checklist y se asigna un 10% para evaluar este parámetro.

Motivación de los equipos técnicos y no técnicos para enfrentar el evento

Este parámetro es importante, ya que la motivación del personal, depende mucho de tener un trabajo eficiente o un trabajo eficaz, y tiene que ver con la confianza que estos tengas sobre su líder y en sí mismos para la aplicación del plan de contingencia y utilizar sus conocimientos y experiencia ante las adversidades presentadas durante la ejecución del plan de contingencia. Se elaboraría un checklist y se asigna un 30% para evaluar este parámetro.

Conocimiento del Plan de contingencia antes ciberataques

La importancia de este parámetro se determina como importante de manera implícita, ya que los equipos tecnológicos deben conocer todo el plan o al menos conocer las tareas que deben ejecutar en su área; si existe desconocimiento o negligencia en la aplicación del plan de contingencia dicha persona no solo se convierte en una dificultad encontrada por el equipo técnico (Punto 1), sino también en una vulnerabilidad que permitiría a la amenaza expandirse en el sistema. Se elaboraría un checklist y se asigna un 30% para evaluar este parámetro.

Procedimientos detallados y documentados

Los procedimientos siempre deben estar documentados y son de vital importancia al momento de aplicar por primera vez el plan de contingencia, luego con las ejecuciones posteriores, servirán de guía de confirmación en la aplicación de los pasos del plan de contingencia. Estos procedimientos deben ser revisados y actualizados de forma constante por el líder de Seguridad Informática. Se elaboraría un checklist y se asigna un 10% para evaluar este parámetro, el cual se muestra en la tabla 21:

PARAMETRO	RESULTADO (SI/NO)	PORCENTAJE (REAL/ESPERADO)		OBSERVACIONES
Presencia de líder de área			4%	
Presencia del Backup del área			4%	
Estación de trabajo disponible			4%	
Ejecución de tareas del área satisfactoriamente			4%	
Atención total del personal hacia el plan de contingencia			4%	
TOTAL			20%	
Problemas en enlaces hacia el CDV			2%	
Enrutamiento en equipos de proveedores de enlace			2%	

Atención satisfactoria de los proveedores (no del CDV)			2%	
Disponibilidad del CDV por parte del proveedor			2%	
Accesos al CLOUD			2%	
TOTAL			10%	
Estabilidad de personal técnico			5%	
Estabilidad de personal no técnico			5%	
Premios por rendimiento			7%	
Personal disciplinado			7%	
Valoración del personal en general			6%	
TOTAL			30%	
Conocer el plan de contingencia			5%	
Conocer tareas propias del área			5%	
Dominar tareas propias del área			10%	
Conocer tareas de otras áreas			3%	

Entender impacto de un ciberataque			7%	
TOTAL			30%	
Manuales versión actual			2%	
Conocer manual general para aplicar plan de contingencia			1%	
Conocer manual del área para aplicar plan de contingencia			3%	
Entender procedimientos de forma detallada			3%	
Mejorar aplicación de tareas del plan de contingencia debido a los manuales			1%	
TOTAL			10%	

Tabla 21 Checklist para evaluar aspectos posibles amenazas al plan de contingencia

El checklist de la tabla 21, debe ser ejecutado en cada área y con dichos resultados realizar una ponderación de forma general, para saber el impacto en la aplicación del Plan de Contingencia ante ciberataques, desde un ámbito controlado. Se debe realizar la misma evaluación con un evento fortuito.

El resultado esperado es un 100%, pero en la práctica podemos considerar un porcentaje satisfactorio desde 85%, ya que el checklist realizado evalúa la parte

humana del equipo de tecnología, porque de ellos dependerá el éxito o fracaso de la aplicación del plan de contingencia; durante la primera ejecución, podemos obtener resultados desde un 50%, esto en el tiempo se irá afinando hasta obtener una ponderación virtual de 90%-100%, siempre debemos tratar de minimizar los inconvenientes controlables (dentro de la empresa), porque si existiesen inconvenientes que no se puede controlar (fuera de la empresa), se podrá mantener una estadística buena de ejecución.

Para realizar el gráfico en el tiempo se establecen los ejes:

- EJE X: Resultado esperado
- EJE Y: Resultado real

Esta gráfica nos indicará la curva de aprendizaje y posteriormente el rendimiento del personal sobre la aplicación del plan de contingencia ante ciberataques.

Se efectuará el escenario antes descrito en la sección 6.5; se asumirá que el checklist fue llenado por cada área, se ha recopilado y registrado, por parte de los líderes de área las ponderaciones para obtener un resultado general (tabla 22):

PARAMETRO	RESULTADO (SI/NO)	PORCENTAJE (REAL/ESPERADO)		OBSERVACIONES
Presencia de líder de área	SI	4%	4%	
Presencia del Backup del área	SI	4%	4%	
Estación de trabajo disponible	SI	4%	4%	
Ejecución de tareas del área satisfactoriamente	SI	2%	4%	Parcialmente
Atención total del personal hacia el plan de	SI	1%	4%	Parcialmente

contingencia				
TOTAL		15%	20%	
Problemas en enlaces hacia el CDV	NO	2%	2%	
Enrutamiento en equipos de proveedores de enlace	SI	1%	2%	Parcialmente
Atención satisfactoria de los proveedores (no del CDV)	NO	0%	2%	La prioridad del Proveedor no fue óptima
Disponibilidad del CDV por parte del proveedor	SI	2%	2%	
Accesos al CLOUD	SI	1%	2%	Problemas con claves
TOTAL		6%	10%	
Estabilidad de personal técnico	SI	5%	5%	
Estabilidad de personal no técnico	SI	5%	5%	
Premios por rendimiento	SI	5%	7%	Se otorgan por rotación según código interno de la empresa
Personal disciplinado	SI	3%	7%	Solo parte del equipo de tecnología
Valoración del	SI	4%	6%	Parcialmente

personal en general				
TOTAL		22%	30%	
Conocer el plan de contingencia	SI	3%	5%	Solo lo conocen parcialmente
Conocer tareas propias del área	SI	5%	5%	
Dominar tareas propias del área	SI	7%	10%	No dominan las tareas del área, existen dudas en aplicarlas
Conocer tareas de otras áreas	SI	2%	3%	Se conocen solo por nombre, pero no su significado
Entender impacto de un ciberataque	SI	5%	7%	Se entiende significado de ciberataque, pero no su impacto
TOTAL		22%	30%	
Manuales versión actual	SI	2%	2%	
Conocer manual general para aplicar plan de contingencia	SI	1%	1%	
Conocer manual del área para aplicar plan de contingencia	SI	2%	3%	Existe dependencia al manual, debido a dudas en aplicación del plan
Entender procedimientos de forma	SI	2%	3%	Se conocen y aplican, pero no entienden los

detallada				procedimientos
Mejorar aplicación de tareas del plan de contingencia debido a los manuales	SI	1%	1%	Se alacrán dudas cuando se lleva el plan a la practica
TOTAL		8%	10%	
RESULTADO TOTAL		**73%**	**100%**	

Tabla 22 Checklist evaluando las amenazas del plan de contingencia

La tabla 22 muestra la evaluación de cada área y ha determinado que el plan de contingencia ante ciberataques solo será efectivo si el personal que debe realizarlo se encuentra altamente comprometido con la empresa, siguiendo esta línea, la empresa debe cuidar de su personal, ya que solo así sentirán el deber de trabajar no solo para el sueldo, sino para que la empresa crezca. El plan de contingencia ante ciberataques que se ha presentado es una guía general que cualquier empresa o institución pública puede aplicar a sus sistemas, considerando los cambios que deban realizarse de acuerdo a su infraestructura y tipo de negocio. El plan de contingencia ante ciberataques es práctico y posee lineamientos generales, se ha concebido para que sea administrado como un proyecto de mejora continua, y su aplicación 2 veces al año. No se ha adentrado en cuestiones técnicas específicas porque dichas cuestiones son variables en cada empresa o institución, pero este como cualquier plan, su éxito o fracaso depende de la motivación que tenga el personal para con la empresa y viceversa. La presente evaluación ha dado como resultado un 73% de efectividad,, es decir la ejecución por primera vez por parte del personal ha estado en una calificación por encima del 70%, es decir, hubieron problemas al momento de ejecutarse, por desconocimiento parcial del procedimiento, inexperiencia y problemas con el proveedor del servicio de CDV, sin embargo, esto nos provee una curva de aprendizaje que ayudará a alcanzar el 90%-100% de efectividad, el punto de inflexión seria de 85%, ya que a menor porcentaje,

significan más problemas presentados y la empresa sufriría un impacto económico severo.

La tabla 23 muestra un ejemplo de ejecuciones sucesivas del plan de contingencia de forma teórica y la figura 6.6 muestra la línea de tiempo de las ejecuciones y sus resultados de efectividad:

EJECUCIONES DEL PLAN	RESULTADO
PRIMERA EJECUCION	73%
SEGUNDA EJECUCION	80%
TERCERA EJECUCION	85%
CUARTA EJECUCION	90%
QUINTA EJECUCION	95%

Tabla 23 Cuadro de ejecuciones del plan de contingencia y sus resultados teóricos

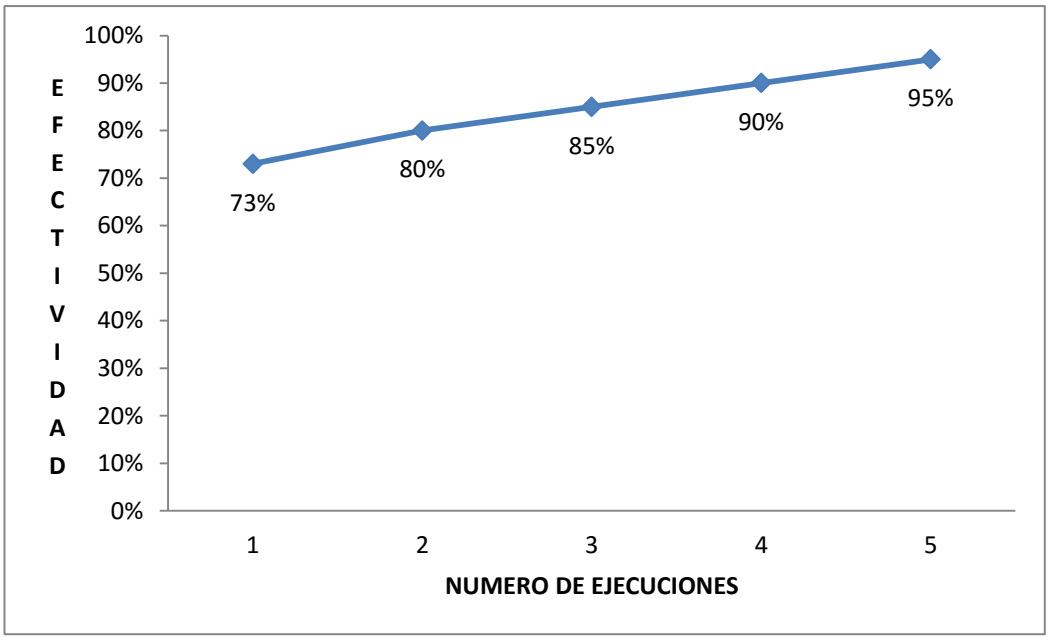


Figura 6.6 Resultados de ejecuciones teóricas del plan de contingencia y su efectividad

CONCLUSIONES Y RECOMENDACIONES

El plan de contingencia ante ciberataques es un proyecto que las empresas deben realizar y aplicar, porque los negocios han migrado a Internet y sin las seguridades necesarias no solo para evitar las amenazas sino para actuar cuando estén presentes en el sistema, las empresas podrían enfrentar desde robos de información, problemas judiciales hasta el cese de operaciones por bancarrota.

Se concluye que los planes de contingencia ante ciberataques, por lo antes expuesto, deben ser considerados con la misma importancia como los desastres naturales, porque ambos son destructivos, con la particularidad que los ciberataques generan robos de información, borrado de discos duros, indisponibilidad de servicios muchas veces realizados por empresas competidoras. Se puede elaborar el mejor plan de contingencia, tomando en cuenta todos los factores por donde pueda fallar, pero si no se cuida la motivación del personal de la empresa, será un fracaso porque los compromisos y lealtades no pueden planificarse ni comprarse, solo se obtienen cuando ambos trabajan y cuidan uno del otro.

Se recomienda que los planes de contingencia (de cualquier índole) sean aplicados al menos 2 veces al año; la primera ejecución del plan es crítica, porque será un indicador sobre los conocimientos que el personal tiene no solo sobre la ejecución del plan, sino sobre las acciones de su área y demás áreas dependientes, donde si presentan falencias, el compromiso es ir mejorando continuamente hasta alcanzar un grado de automatización en las tareas necesarias del plan y un aumento de conocimiento acerca de sus tareas propias del día a día.

BIBLIOGRAFÍA

[1] Hyponnen Mikko Ciberataques, artículo publicado en el blog tecnológico OpenMind, noviembre del 2016

[2] Ureña Centeno Fransisco Ciberataques, la mayor amenaza actual, IEEE, documento de opinión del 16 de enero 2015.

[3] María José Vigo Jaccottet, Carlos Alberto Cardoso Flores, Wilson Adrián de Mello Cabrera, PLANES DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO, Monografía para Contador Público PLAN 90 de la Universidad de la República, Marzo 2010.

[4] Gaspar Martínez Juan, PLAN DE CONTINGENCIAS: ELABORACION, DESARROLLO Y GESTION, Ediciones Dias de Santos, 2004.

[5] Dejan Kosutic Ciberseguridad en 9 pasos, EPPS Services Ltd, Zagreb, 2012

[6] Rodrigo Herrero Pizarro, PLANES DE CONTINGENCIA Y SU AUDITORÍA, Proyecto de fin de carrera de la Universidad Carlos III de Madrid, mayo 2010.

[7] Secretaria Nacional de la Administración Pública de Ecuador, ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION EGSI, Acuerdo ministerial 166, publicado en el Registro Oficial suplemento 88 del 25 de septiembre del 2013.

[8] ISO 22301:2012, Seguridad de Sociedad: Sistemas de Continuidad del Negocio-Requisitos; mayo 2012.

[9] Instituto del Mar del Perú, PLAN DE CONTINGENCIA INFORMÁTICO, Resolución Directoral N° DE-158-2012, agosto 2012.

[10] Augusto Cabrera Duffaut, ESTUDIO PARA LA IMPLEMENTACION DE DATACENTER BASADOS EN EL MODELO CLOUD COMPUTING, Tesis Postgrado de la Universidad de Cuenca, septiembre 2013.

[11] Eduardo Gallego, Jorge E. López de Vergara, Honeynets: Aprendiendo del Atacante, Libro de Ponencias del IX Congreso Nacional de Internet, Telecomunicaciones y Movilidad (MUNDO INTERNET 2004) realizado en Madrid, 11-13 de febrero 2004. Depósito legal M-5613-2004.

[12] Miguel Angel García, Calculando la disponibilidad de sistemas complejos, junio 2015.

[13] Guido Rosales Uriona, Las peores brechas de seguridad del siglo XXI, febrero 2012.

ANEXOS

Anexo 1: GLOSARIO

Amenaza: Todo evento que se considere peligroso para el sistema o la empresa.

Bots: Se origina de robot, se define como todo equipo informático (Computadora) que realiza tareas específicas sin necesidad de un usuario.

Centro de Datos: Agrupación de equipos servidores, comunicaciones y demás para realizar la captación, procesamiento y almacenamiento de datos, generalmente son equipados con climatización controlada y seguridades estrictas.

Centro de Datos Virtual: Similar a la definición de Centro de Datos, con la particularidad que se ubica en la nube, la infraestructura depende de un proveedor.

Checklist: Se define como lista de verificación, donde se ingresan parámetros a ser revisados y confirmados en presencia u operación.

Ciberataque: Se denomina a todo ataque o amenaza que involucre o comprometa la integridad de un sistema o grupo de sistemas de empresas o grupo de empresas.

Ciberincidente: Se denomina todo evento ejecutado en la red o el sistema.

Cloud (Nube): Termino utilizado para indentificar servicio ofrecido por empresas a través de internet o enlaces de datos privados.

Cobit: Se refiere a la guía de mejores prácticas utilizadas por una empresa; dirigida al control y supervisión de tecnología de la información (TI).

Community Manager: Se define como tal a la persona que administra redes sociales de una empresa.

Contingencia: Se define como contingencia a los eventos posibles por suceder, pero sin la certeza de que ello ocurra alguna vez.

DDoS: Ataque de Denegación de Servicio Distribuido, son las acciones que inhabilitan un servicio en la red.

Elastix: Plataforma basada en CentOS y Asterisk que ofrece servicio de telefonía IP.

Enlace de datos: Conexión física y lógica de red punto a punto o multipunto ofrecidos por un proveedor.

Exploit: Son acciones que aprovechan las vulnerabilidades de un sistema para obtener un comportamiento anormal.

F5 (WAF): Firewall de aplicativos web que también funciona como balanceador de carga, es ofrecido por la empresa F5.

Feedback: Se define como feedback, a la retroalimentación de resultados esperados o no esperados de un sistema o proyecto.

Firewall: Equipo informático de red que ofrece protección media y alta contra ataques e intrusiones mediante reglas. Estos equipos pueden ser vulnerados solo por expertos y botnets.

Hacker: Persona o agrupación que se dedican a vulnerar Sistemas para obtener información. Dependiendo de la intención y el resultado de sus acciones pueden ser considerados delincuentes.

Honeynet: Herramienta de seguridad informática ubicada en la red diseñada para ser el objetivo de ataques informáticos para detectarlos, obtener información de ellos y mitigarlos.

INRow: Termino utilizado por equipos de climatización tipo rack.

IPS: Equipo de seguridad informática que se caracteriza por prevenir intrusiones no autorizadas, estos equipos pueden ser vulnerados por expertos y botnets.

ISO: Referencia a la Organización Internacional de Normalización.

Pentesting: Referencia a las pruebas de penetración en un sistema para detectar vulnerabilidades.

Servidor: Equipo informático, diseñado para procesamiento de altas prestaciones.

Sistema: Agrupación de servidores, equipos de red, orientados al procesamiento y almacenamiento de información ubicados generalmente en un centro de datos.

SLA: Referencia al Acuerdo de Nivel de Servicio (Service Layer Agreement) entre un proveedor y sus clientes.

Spam: Correos no deseados, generalmente utilizados por ingeniería social para inyección de código malicioso.

Storage: Referencia al almacenamiento de datos masivos en forma de arreglo de discos.

Streaming: Referencia a servicios de transmisión multimedia (audio y video) en tiempo real ofrecidos a través de internet.

Switch: Equipo de red que interconecta usuarios, servidores u otros equipos de red a través de cobre o fibra óptica mediante las direcciones MAC.

Transacción Electrónica: Referencia a la transferencia de información digital que se efectúa entre dos partes mediante un medio de red.

Virus Informático: Software que contiene código malicioso que al momento de ejecutarse, la serie de acciones programadas en el generan un comportamiento anormal en su huésped (computadora, servidor, Smartphone, etc).

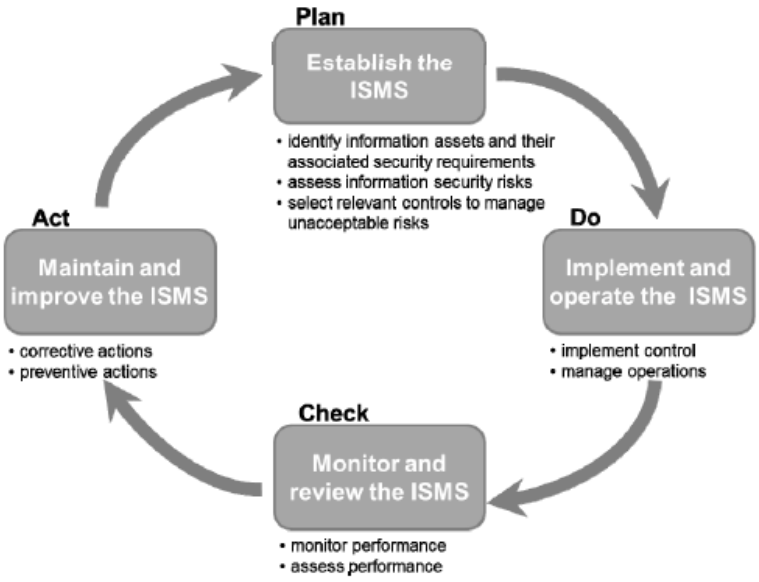
VPN: Referencia a Red Privada Virtual (Virtual Private Network), enlaza dos redes privadas a través del internet sin comprometer la integridad de la información.

Webservice: Conjunto de protocolos y tecnologías que sirven para intercambiar información entre aplicaciones via internet, enlace de datos dedicado, red local o conexiones seguras de red.

Anexo 2: Imágenes sobre la base de Cobit e ISO 27001, sobre planes de contingencia y seguridad de la información respectivamente.

Figura Anexo 1: Procesos de Cobit para planes de contingencia

Figura Anexo 1.1: Procesos de ISO 27001 para garantizar la seguridad de la información



Anexo 3: Breve información acerca de Honeynets, tomado del Documento: "Honeynets: Aprendiendo del Atacante", Autores: Eduardo Gallego, Jorge E. López de Vergara, en febrero 2004.

Honeynets

Una honeynet es una herramienta de seguridad diseñada para ser sondeada, atacada y comprometida por un hipotético intruso. Se trata de una red completa, compuesta por un conjunto de sistemas dispuestos a recibir estos ataques y una serie de mecanismos encargados de la monitorización, el registro y el control de estas acciones. Es una especie de pecera, en cuyo interior se puede observar al atacante en su hábitat natural.

Mediante el estudio del comportamiento de los intrusos durante el sondeo, el ataque y el compromiso de los sistemas de la honeynet y el análisis de su posterior actividad en el interior de los sistemas comprometidos, es posible aprender sobre las tácticas y los motivos de la comunidad de atacantes que puebla Internet. Esta ponencia presenta a las honeynets como el honeypot más potente, analiza las distintas propuestas existentes y hace énfasis en la virtualización de este tipo de herramienta.

Durante los últimos años las intrusiones y los ataques informáticos a través de Internet se han incrementado notablemente. Este incremento en el número de incidentes ha venido acompañado por una clara evolución de las herramientas y técnicas utilizadas por los atacantes. Parte de los responsables de estas acciones son usuarios avanzados que desarrollan sus propias aplicaciones y son capaces de crear y utilizar sofisticadas puertas traseras para introducirse en otros sistemas. Estos individuos son los más cercanos a la figura del hacker que tiene la opinión pública: expertos en informática, seguridad y redes de ordenadores, capaces de entrar en el ordenador más protegido de la compañía más importante, aunque para ello tengan que saltarse las medidas de seguridad más complejas. Esta idea generalizada y en muchos casos mitificada sobre el perfil de estos intrusos hace pensar que sólo serán objeto de ataque aquellos equipos que contengan información trascendente. Sin embargo, esto es un grave error. Estos ataques selectivos dirigidos por expertos suponen un porcentaje muy pequeño de los que a

diario se producen a través de La red. La práctica totalidad de los incidentes que acontecen en Internet no van dirigidos contra equipos ni compañías específicas, sino que tienen como objetivo la víctima fácil. El blanco seleccionado puede ser cualquier equipo conectado a La Red que posea una debilidad específica que el atacante busca y es capaz de aprovechar para conseguir el acceso a la máquina.

Por otro lado, hoy ya no se necesita poseer unos conocimientos desbordantes sobre el funcionamiento de un sistema para poder atacarlo.

De hecho, la mayoría de los intrusos se limita a utilizar herramientas creadas por otros, herramientas que se pueden encontrar fácilmente en Internet, que son cada vez más sencillas de manejar y que no exigen que el atacante conozca su modo interno de funcionamiento. Basta con que ejecute un simple comando o introduzca una serie de instrucciones que en muchas ocasiones se detallan al inicio del propio código de los programas o se incluyen en ficheros de texto que acompañan a las aplicaciones. En los últimos años, la frecuencia de aparición de estos ataques indiscriminados se ha disparado,y este hecho, unido al creciente número de vulnerabilidades descubiertas en todo tipo de sistemas operativos y aplicaciones, convierte a cualquier sistema conectado a Internet en una víctima potencial. Este panorama plantea la necesidad de disponer de instrumentos que permitan descubrir y analizar tanto los agujeros de seguridad que pueda presentar un sistema como las técnicas y herramientas utilizadas por la comunidad de atacantes que puebla la red.

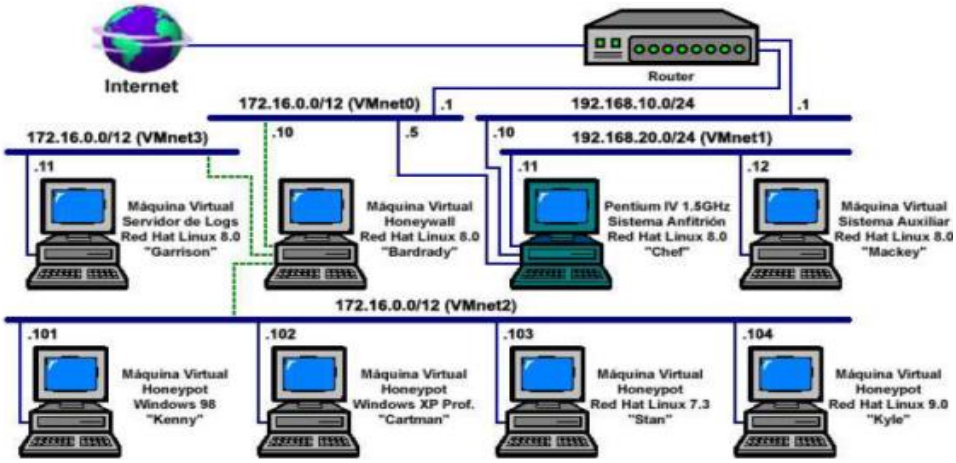


Figura Anexo 2 Diagrama de Honeynet

Anexo 4: Formulario para control de seguridad de información, tomado de la norma ISO 27001

Control objectives and controls

The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 17799:2005 Clauses 5 to 15. The lists in Table A.1 are not exhaustive and an organization may consider that additional control objectives and controls are necessary. Control objectives and controls from these tables shall be selected as part of the ISMS process specified in 4.2.1.

ISO/IEC 17799:2005 Clauses 5 to 15 provide implementation advice and guidance on best practice in support of the controls specified in A.5 to A.15.

Table A.1 – Control objectives and controls

A.5 Security policy		
A.5.1 Information security policy *Objective:* To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	Information security policy document	*Control* An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.
A.5.1.2	Review of the information security policy	*Control* The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
A.6 Organization of information security		
A.6.1 Internal organization *Objective:* To manage information security within the organization.		
A.6.1.1	Management commitment to information security	*Control* Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
A.6.1.2	Information security co-ordination	*Control* Information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.
A.6.1.3	Allocation of information security responsibilities	*Control* All information security responsibilities shall be clearly defined.

A.6.1.4	Authorization process for information processing facilities	*Control* A management authorization process for new information processing facilities shall be defined and implemented.
A.6.1.5	Confidentiality agreements	*Control* Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.
A.6.1.6	Contact with authorities	*Control* Appropriate contacts with relevant authorities shall be maintained.
A.6.1.7	Contact with special interest groups	*Control* Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
A.6.1.8	Independent review of information security	*Control* The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.
A.6.2 External parties *Objective:* To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.		
A.6.2.1	Identification of risks related to external parties	*Control* The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
A.6.2.2	Addressing security when dealing with customers	*Control* All identified security requirements shall be addressed before giving customers access to the organization's information or assets.
A.6.2.3	Addressing security in third party agreements	*Control* Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.

A.7 Asset management		
A.7.1 Responsibility for assets *Objective:* To achieve and maintain appropriate protection of organizational assets.		
A.7.1.1	Inventory of assets	*Control* All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.
A.7.1.2	Ownership of assets	*Control* All information and assets associated with information processing facilities shall be 'owned' [3] by a designated part of the organization.
A.7.1.3	Acceptable use of assets	*Control* Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.
A.7.2 Information classification *Objective:* To ensure that information receives an appropriate level of protection.		
A.7.2.1	Classification guidelines	*Control* Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.
A.7.2.2	Information labelling and handling	*Control* An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.
A.8 Human resources security		
A.8.1 Prior to employment [4] *Objective:* To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.		
A.8.1.1	Roles and responsibilities	*Control* Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.

A.8.1.2	Screening	*Control* Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
A.8.1.3	Terms and conditions of employment	*Control* As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.
A.8.2 During employment *Objective:* To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.		
A.8.2.1	Management responsibilities	*Control* Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.
A.8.2.2	Information security awareness, education and training	*Control* All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
A.8.2.3	Disciplinary process	*Control* There shall be a formal disciplinary process for employees who have committed a security breach.
A.8.3 Termination or change of employment *Objective:* To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.		
A.8.3.1	Termination responsibilities	*Control* Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.
A.8.3.2	Return of assets	*Control* All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.
A.8.3.3	Removal of access rights	*Control* The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

A.9 Physical and environmental security		
A.9.1 Secure areas *Objective:* To prevent unauthorized physical access, damage and interference to the organization's premises and information.		
A.9.1.1	Physical security perimeter	*Control* Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.
A.9.1.2	Physical entry controls	*Control* Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.9.1.3	Securing offices, rooms and facilities	*Control* Physical security for offices, rooms, and facilities shall be designed and applied.
A.9.1.4	Protecting against external and environmental threats	*Control* Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.
A.9.1.5	Working in secure areas	*Control* Physical protection and guidelines for working in secure areas shall be designed and applied.
A.9.1.6	Public access, delivery and loading areas	*Control* Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
A.9.2 Equipment security *Objective:* To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.		
A.9.2.1	Equipment siting and protection	*Control* Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
A.9.2.2	Supporting utilities	*Control* Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
A.9.2.3	Cabling security	*Control* Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

A.9.2.4	Equipment maintenance	*Control* Equipment shall be correctly maintained to ensure its continued availability and integrity.
A.9.2.5	Security of equipment off-premises	*Control* Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.
A.9.2.6	Secure disposal or re-use of equipment	*Control* All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
A.9.2.7	Removal of property	*Control* Equipment, information or software shall not be taken off-site without prior authorization.
A.10 Communications and operations management		
A.10.1 Operational procedures and responsibilities *Objective:* To ensure the correct and secure operation of information processing facilities.		
A.10.1.1	Documented operating procedures	*Control* Operating procedures shall be documented, maintained, and made available to all users who need them.
A.10.1.2	Change management	*Control* Changes to information processing facilities and systems shall be controlled.
A.10.1.3	Segregation of duties	*Control* Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
A.10.1.4	Separation of development, test and operational facilities	*Control* Development, test and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.
A.10.2 Third party service delivery management *Objective:* To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.		
A.10.2.1	Service delivery	*Control* It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

A.10.2.2	Monitoring and review of third party services	*Control* The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.
A.10.2.3	Managing changes to third party services	*Control* Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.
A.10.3 System planning and acceptance *Objective*: To minimize the risk of systems failures.		
A.10.3.1	Capacity management	*Control* The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.
A.10.3.2	System acceptance	*Control* Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.
A.10.4 Protection against malicious and mobile code *Objective*: To protect the integrity of software and information.		
A.10.4.1	Controls against malicious code	*Control* Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.
A.10.4.2	Controls against mobile code	*Control* Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.
A.10.5 Back-up *Objective*: To maintain the integrity and availability of information and information processing facilities.		
A.10.5.1	Information back-up	*Control* Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.

A.10.6 Network security management *Objective:* To ensure the protection of information in networks and the protection of the supporting infrastructure.		
A.10.6.1	Network controls	*Control* Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
A.10.6.2	Security of network services	*Control* Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.
A.10.7 Media handling *Objective:* To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.		
A.10.7.1	Management of removable media	*Control* There shall be procedures in place for the management of removable media.
A.10.7.2	Disposal of media	*Control* Media shall be disposed of securely and safely when no longer required, using formal procedures.
A.10.7.3	Information handling procedures	*Control* Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.
A.10.7.4	Security of system documentation	*Control* System documentation shall be protected against unauthorized access.
A.10.8 Exchange of information *Objective:* To maintain the security of information and software exchanged within an organization and with any external entity.		
A.10.8.1	Information exchange policies and procedures	*Control* Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.
A.10.8.2	Exchange agreements	*Control* Agreements shall be established for the exchange of information and software between the organization and external parties.
A.10.8.3	Physical media in transit	*Control* Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.

A.10.8.4	Electronic messaging	*Control* Information involved in electronic messaging shall be appropriately protected.
A.10.8.5	Business information systems	*Control* Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.
A.10.9 Electronic commerce services *Objective:* To ensure the security of electronic commerce services, and their secure use.		
A.10.9.1	Electronic commerce	*Control* Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.
A.10.9.2	On-line transactions	*Control* Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
A.10.9.3	Publicly available information	*Control* The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.
A.10.10 Monitoring *Objective:* To detect unauthorized information processing activities.		
A.10.10.1	Audit logging	*Control* Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
A.10.10.2	Monitoring system use	*Control* Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.
A.10.10.3	Protection of log information	*Control* Logging facilities and log information shall be protected against tampering and unauthorized access.
A.10.10.4	Administrator and operator logs	*Control* System administrator and system operator activities shall be logged.
A.10.10.5	Fault logging	*Control* Faults shall be logged, analyzed, and appropriate action taken.

A.10.10.6	Clock synchronization	*Control* The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.
A.11 Access control		
A.11.1 Business requirement for access control *Objective*: To control access to information.		
A.11.1.1	Access control policy	*Control* An access control policy shall be established, documented, and reviewed based on business and security requirements for access.
A.11.2 User access management *Objective*: To ensure authorized user access and to prevent unauthorized access to information systems.		
A.11.2.1	User registration	*Control* There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.
A.11.2.2	Privilege management	*Control* The allocation and use of privileges shall be restricted and controlled.
A.11.2.3	User password management	*Control* The allocation of passwords shall be controlled through a formal management process.
A.11.2.4	Review of user access rights	*Control* Management shall review users' access rights at regular intervals using a formal process.
A.11.3 User responsibilities *Objective*: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.		
A.11.3.1	Password use	*Control* Users shall be required to follow good security practices in the selection and use of passwords.
A.11.3.2	Unattended user equipment	*Control* Users shall ensure that unattended equipment has appropriate protection.
A.11.3.3	Clear desk and clear screen policy	*Control* A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

A.11.4 Network access control *Objective:* To prevent unauthorized access to networked services.		
A.11.4.1	Policy on use of network services	*Control* Users shall only be provided with access to the services that they have been specifically authorized to use.
A.11.4.2	User authentication for external connections	*Control* Appropriate authentication methods shall be used to control access by remote users.
A.11.4.3	Equipment identification in networks	*Control* Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.
A.11.4.4	Remote diagnostic and configuration port protection	*Control* Physical and logical access to diagnostic and configuration ports shall be controlled.
A.11.4.5	Segregation in networks	*Control* Groups of information services, users, and information systems shall be segregated on networks.
A.11.4.6	Network connection control	*Control* For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications (see 11.1).
A.11.4.7	Network routing control	*Control* Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
A.11.5 Operating system access control *Objective:* To prevent unauthorized access to operating systems.		
A.11.5.1	Secure log-on procedures	*Control* Access to operating systems shall be controlled by a secure log-on procedure.
A.11.5.2	User identification and authentication	*Control* All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
A.11.5.3	Password management system	*Control* Systems for managing passwords shall be interactive and shall ensure quality passwords.

A.11.5.4	Use of system utilities	*Control* The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
A.11.5.5	Session time-out	*Control* Inactive sessions shall shut down after a defined period of inactivity.
A.11.5.6	Limitation of connection time	*Control* Restrictions on connection times shall be used to provide additional security for high-risk applications.
A.11.6 Application and information access control *Objective:* To prevent unauthorized access to information held in application systems.		
A.11.6.1	Information access restriction	*Control* Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.
A.11.6.2	Sensitive system isolation	*Control* Sensitive systems shall have a dedicated (isolated) computing environment.
A.11.7 Mobile computing and teleworking *Objective:* To ensure information security when using mobile computing and teleworking facilities.		
A.11.7.1	Mobile computing and communications	*Control* A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.
A.11.7.2	Teleworking	*Control* A policy, operational plans and procedures shall be developed and implemented for teleworking activities.
A.12 Information systems acquisition, development and maintenance		
A.12.1 Security requirements of information systems *Objective:* To ensure that security is an integral part of information systems.		
A.12.1.1	Security requirements analysis and specification	*Control* Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.

A.12.2 Correct processing in applications *Objective:* To prevent errors, loss, unauthorized modification or misuse of information in applications.		
A.12.2.1	Input data validation	*Control* Data input to applications shall be validated to ensure that this data is correct and appropriate.
A.12.2.2	Control of internal processing	*Control* Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
A.12.2.3	Message integrity	*Control* Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.
A.12.2.4	Output data validation	*Control* Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
A.12.3 Cryptographic controls *Objective:* To protect the confidentiality, authenticity or integrity of information by cryptographic means.		
A.12.3.1	Policy on the use of cryptographic controls	*Control* A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
A.12.3.2	Key management	*Control* Key management shall be in place to support the organization's use of cryptographic techniques.
A.12.4 Security of system files *Objective:* To ensure the security of system files.		
A.12.4.1	Control of operational software	*Control* There shall be procedures in place to control the installation of software on operational systems.
A.12.4.2	Protection of system test data	*Control* Test data shall be selected carefully, and protected and controlled.
A.12.4.3	Access control to program source code	*Control* Access to program source code shall be restricted.

A.12.5 Security in development and support processes		
Objective: To maintain the security of application system software and information.		
A.12.5.1	Change control procedures	*Control* The implementation of changes shall be controlled by the use of formal change control procedures.
A.12.5.2	Technical review of applications after operating system changes	*Control* When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
A.12.5.3	Restrictions on changes to software packages	*Control* Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.
A.12.5.4	Information leakage	*Control* Opportunities for information leakage shall be prevented.
A.12.5.5	Outsourced software development	*Control* Outsourced software development shall be supervised and monitored by the organization.
A.12.6 Technical Vulnerability Management		
Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.		
A.12.6.1	Control of technical vulnerabilities	*Control* Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.
A.13 Information security incident management		
A.13.1 Reporting information security events and weaknesses		
Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.		
A.13.1.1	Reporting information security events	*Control* Information security events shall be reported through appropriate management channels as quickly as possible.
A.13.1.2	Reporting security weaknesses	*Control* All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

A.13.2 Management of information security incidents and improvements *Objective:* To ensure a consistent and effective approach is applied to the management of information security incidents.		
A.13.2.1	Responsibilities and procedures	*Control* Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
A.13.2.2	Learning from information security incidents	*Control* There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.
A.13.2.3	Collection of evidence	*Control* Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).
A.14 Business continuity management		
A.14.1 Information security aspects of business continuity management *Objective:* To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.		
A.14.1.1	Including information security in the business continuity management process	*Control* A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.
A.14.1.2	Business continuity and risk assessment	*Control* Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.
A.14.1.3	Developing and implementing continuity plans including information security	*Control* Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
A.14.1.4	Business continuity planning framework	*Control* A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.
A.14.1.5	Testing, maintaining and re-assessing business continuity plans	*Control* Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

A.15 Compliance		
A.15.1 Compliance with legal requirements *Objective:* To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.		
A.15.1.1	Identification of applicable legislation	*Control* All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.
A.15.1.2	Intellectual property rights (IPR)	*Control* Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
A.15.1.3	Protection of organizational records	*Control* Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
A.15.1.4	Data protection and privacy of personal information	*Control* Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.
A.15.1.5	Prevention of misuse of information processing facilities	*Control* Users shall be deterred from using information processing facilities for unauthorized purposes.
A.15.1.6	Regulation of cryptographic controls	*Control* Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
A.15.2 Compliance with security policies and standards, and technical compliance *Objective:* To ensure compliance of systems with organizational security policies and standards.		
A.15.2.1	Compliance with security policies and standards	*Control* Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
A.15.2.2	Technical compliance checking	*Control* Information systems shall be regularly checked for compliance with security implementation standards.

A.15.3 Information systems audit considerations *Objective:* To maximize the effectiveness of and to minimize interference to/from the information systems audit process.		
A.15.3.1	Information systems audit controls	*Control* Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
A.15.3.2	Protection of information systems audit tools	*Control* Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

Anexo 5: Encuesta de problemas en equipos informáticos para soporte técnico

Problemas con equipos informáticos de usuarios

1) Liste los signos de un computador con problemas (no virus)

2) Liste los signos de un computador infectado con código malicioso (virus)

3) Liste las acciones a realizar cuando se detecte un computador infectado

4) Escriba el protocolo de escalamiento cuando se encuentre un computador infectado con virus

5) Escriba las vías de propagación de virus más comunes