DISEÑO Y ESTABLECIMIENTO DE CONTROLES DE SEGURIDAD PARA RECUPERACIÓN DE DATOS EN CASO DE DESASTRE BAJO PROTOCOLO IPV6

CÉSAR AUGUSTO CABRERA GARCÍA

ilae
Instituto Latinoamericano de Altos Estudios

Diseño y establecimiento de controles de seguridad para recuperación de datos en caso de desastre bajo protocolo IPv6

Diseño y establecimiento de controles de seguridad para recuperación de datos en caso de desastre bajo protocolo IPv6

César Augusto Cabrera García

Instituto Latinoamericano de Altos Estudios –ILAE–

Publicación sometida a evaluación de pares académicos (*Peer Review Double Blinded*).

ISBN 978-958-5535-85-5

Cra. 18 # 39A-46, Teusaquillo, Bogotá, Colombia
PBX: (571) 232-3705, FAX (571) 323 2181
www.ilae.edu.co

Diseño de carátula y composición: Jesús Alberto Chaparro Tibaduiza
Edición electrónica: Editorial Milla Ltda. (571) 702 1144
editorialmilla@telmex.net.co

Editado en Colombia
Published in Colombia

Dedicatoria

A Dios: porque siempre estuviste a mi lado. Nunca me quejare de lo que me das; siempre estaré agradecido.

A mi Familia, que es un pilar importante en mi vida, pues con su fuerza y coraje muestran que debo luchar para conseguir mis sueños.

Contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS Y GRÁFICOS

Acrónimos

3DES	Triple Data Encryption Standard
AAA	Autenticación, Autorización y Auditoría
ACL	Access Control List
AES	Advanced Encryption Standard
APNIC	Centro de Información de Red de Asia Pacífico
AR	Análisis de Riesgo
ARIN	Registro americano para Números de Internet
ATM	Modo de Transferencia Asincrónico
BCP	Plan de Continuidad del Negocio
BIA	Análisis de Impacto del Negocio
BSD	Berkeley Software Distribution
CA	Autoridad Certificadora
CFP	Centro de Formación Profesional
CP	Contingencia y Plan
CPU	Unidad Central de Procesos
DEPTI	Departamento Tecnología de Información
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	Zona Desmilitarizada
DNS	Sistema de Nombre de dominio
DR	Disaster Recovery
DRP	Disaster Recovery Plan
ERP	Enterprise Resource Planning
FDDI	Fiber Distributed Data Interface
FLAP	FDDI Link Access Protocol
GCN	Gestión de Continuidad de Negocio
GR	Grado de Riesgo
GRE	Generic Routing Encapsulation
IANA	Autoridad de Números Asignación de Internet
IC	Índice de Capacitación

IDEA	International Data Encryption Algorithm
IF	Índice de Frecuencia
IGP	Instituto Geofísico del Perú
INDECI	Instituto Nacional de Defensa Civil
INEI	Instituto Nacional de Estadística e Informática
IP	Protocolo de Internet
IPE	Índice de Persona Expuestas
IPER	Identificación de Peligros, Evaluación de Riesgos
IPR	índice de Procedimientos Existentes
IPSEC	**:** Protocolo de Internet Seguro
IPv6	**:** Protocolo de Internet Versión 6
ISATAP	**:** Protocolo de Dirección de Túnel Automático
ISO	**:** Organización Internacional para la Estandarización
ISO/IEC	Organización Internacional para la Estandarización / Comisión Internacional Electrotécnica
ISP	Proveedores de Servicios de Internet
LACNIC	América Latina y Centro de Información de Red caribeño
LAN	Local Area Network
LDAP	Protocolo Ligero de Acceso a Directorios
MTA	Mail Transfer Agent
MTDL	Longitud de Interrupción Máxima Tolerable
MTPD	Período Máximo Tolerable de Interrupción
P	Probabilidad
P2P	Peer to Peer
PBI	Producto Bruto Interno
PDCA	Planificar, Hacer, Verificar y Actuar
PKI	Infraestructura de Clave Pública
RC2	Rivest Cipher 2
RC4	Rivest Cipher 4
RC5	Rivest Cipher 5
RDSI	Red Digital de Servicios Integrados
RIPE	Registros de Internet Regionales
ROI	Retorno Sobre la Inversión
ROSI	Retorno sobre la Inversión en Seguridad de Información
S	Severidad
SAP	Sistemas, Aplicaciones y Productos
SENAMHI	Servicios Nacional de Meteorología e Hidrología del Perú
SENATI	Servicio Nacional de Adiestramiento en Trabajo Industrial
SGCN	Sistema de Gestión de Continuidad de Negocio
SGSI	Sistema de Gestión de Seguridad de la Información

SINFO	Sistema de Información
SIPP	Protocolo de Internet Simple
SLAAC	Autoconfiguración de Direcciones Libres de Estado
SQL	Lenguaje de Consulta Estructurada
TI	Tecnología de Información
TIC	Tecnología de la Información y la Comunicación
TIR	Tasa Interna de Retorno
UFP	Unidad de Formación Profesional
ULA	Dirección Única Local
VAN	Valor Actual Neto
VOIP	Voz sobre Protocolo de Internet
VPN	Red Privada Virtual
ZOADICA	Zonal Administrativa ICA

Introducción

El plan de recuperación de datos en caso de desastres se ha configurado no solo como un plan de emergencia ante cualquier evento, desastre o circunstancia que llegara a suceder en cualquier latitud, región o localidad. Este plan proporciona de acuerdo a definiciones aportadas por notables investigadores una perspectiva estructurada a las incidencias no establecidas que podrían poner en riesgo la infraestructura, así como proteger de manera total las inversiones realizadas.

Implementar un plan que proteja de manera real el sistema operativo ante cualquier desafuero de la naturaleza, también ante cualquier situación, puede significar, no solo la pérdida de información vital para la organización, sino también puede traducirse en una amenaza que no cesará hasta que el propio sistema esté en su totalidad resguardado. Esto puede entenderse desde una visión mucho más amplia en que este mismo plan pueda crear sus propias lógicas de sentido para generar sus mecanismos, recursos, metodologías y técnicas en caso de presentarse un desastre de cualquier índole.

Algunas de las actividades desfavorables sin duda en materia de eventos, fenómenos, han permitido la generación de propuestas que, en aras de evitar, más bien podrían advertir con un tiempo prudencial a que estas provocaran la anulación y posterior extravío de información u omisión de datos.

En la actualidad muchas son las compañías que se han visto envueltas en desastres o eventos de la naturaleza; y ante la ausencia de un plan de recuperación muchas de estas empresas han tenido que cerrar sus puertas por no tener un sistema o un plan de recuperación de sus datos: se vuelve cuesta arriba concebir hoy por hoy una empresa sin este sistema de seguridad. Sin un plan de esta naturaleza es casi imposible que se recupere.

El plan de Recuperación de Datos que emplea el protocolo IPv6, permite adecuar todo un mecanismo de defensa de manera eficiente ante cualquier tipo de amenaza y que ponga en riesgo datos esenciales para el normal funcionamiento de la organización o empresa. Este protocolo no es solo necesario, sino que la mayoría de las compañías que prestan algún tipo de servicio han visto este sistema como un recurso indispensable para la protección de la información. El protocolo IPv6 es un dispositivo empleado sobre todo para almacenar gran cantidad de información, sin embargo, este protocolo ha reemplazado las funciones de un protector corriente al ganar no solo un puesto en el desplazamiento, y una oportuna respuesta ante los avatares que puede tener la organización, sino que además este protocolo puede direccionar sus datos para un mejor desempeño en aras del desarrollo de la empresa. Este aspecto cobra más importancia en la informática empresarial contemporánea.

Implementar un plan de recuperación ya no es solo un asunto que debe importar a solo un grupo de organizaciones que ofrecen algún tipo de servicio, llámese comunicacional o estratégico, sino que además un plan debe contemplar una serie de aspectos que son fundamentales para el entorno. Para nadie es un secreto que el ser humano se mueve en terrenos donde la tecnología tiene un rol determinante en la configuración organizacional de primer orden. Esto sin contar que la implementación de este tipo de protocolos puede de igual manera generar estadios para el estudio, la sistematización y la producción de otros dispositivos de seguridad que puedan predecir con mayor precisión algún evento o momento donde se manifiesten los daños que en años anteriores era imposible de concebir.

La presente investigación se centró en particular en proponer un plan justo para la recuperación de datos en situaciones de desastre que tal vez ameriten la activación de protocolos de seguridad, así como el diseño de mecanismos que apuntalen a minimizar el sin número de riesgos que atraviesan las organizaciones cuando se hace presente algún evento de cualquier naturaleza, sin que esto signifique que este plan sea solo para la protección sino que también pudiera emplearse con otros propósitos u objetivos.

Capítulo primero
Plan de controles de seguridad de recuperación de desastres en TI: problemática actual

Desde el surgimiento de la tecnología, si bien es cierto que le ha dado a la sociedad un mecanismo para poder comunicarse y buscar información, que resultaba de difícil acceso para el individuo, a través de las redes; también ha surgido la necesidad de poder recabar y guardar esa información en caso que llegase a ocurrir un desastre natural o de otra índole, para así poder recuperar y almacenar la información que se requiere y por la que tanto se ha trabajado. Por ejemplo, los bancos a nivel mundial se manejan a través de un sistema electrónico que recaba la información y las guardan en el sistema operativo de las computadoras o, en tal caso, en la tarjeta madre de algún equipo principal que maneje todas las máquinas; los bancos deben tener un sistema de recuperación de datos en caso de que ocurriera algún desastre para no perder información valiosa para toda la sociedad, puesto que se habla de los sistemas financieros de cada individuo que integra la sociedad y que confía en el banco correspondiente para guardar sus ganancias monetarias.

Es por esto, que, con el surgimiento de la tecnología, también surgen posibles soluciones y factores que determinan la utilidad y el resguardo de la información utilizada por los individuos de la sociedad. Uno de los elementos que permiten la integridad y la seguridad de la tecnología es el Plan de Recuperación de Datos –DRP–, el cual consiste en un plan de emergencia que tiene la capacidad de recuperar la información de la central de datos de alguna organización u entidad de manera inmediata y completa cuando es víctima de un desastre natural o de otra índole. Esta necesidad de crear un plan de emergencia se forma debido al gran impacto que se origina en el progreso

de las labores en una organización debido a una interrupción total o parcial de la estructura de la información y de sus aplicaciones tecnológicas; este plan de recuperación de datos tiene la capacidad de hacer frente a esta eventualidad relacionada con el desarrollo ineficaz de actividades y de los equipos tecnológicos admitiendo el absoluto funcionamiento de los sistemas y de los servicios específicos que se maneja dentro de la organización u entidad. El Plan de Recuperación de Datos permite una estructura gradual para asegurar la infraestructura de TI (personas, procesos tecnológicos, *hardware* y *software*) en caso de ocurrir incidentes que la pongan en peligro. Los incidentes pueden variar, pero los objetivos principales no, las cuales consisten en asegurar la protección de las inversiones elaboradas en la central de datos y en desarrollar la capacidad de los trabajadores para ejecutar las operaciones empresariales.

I. Contextualización mundial

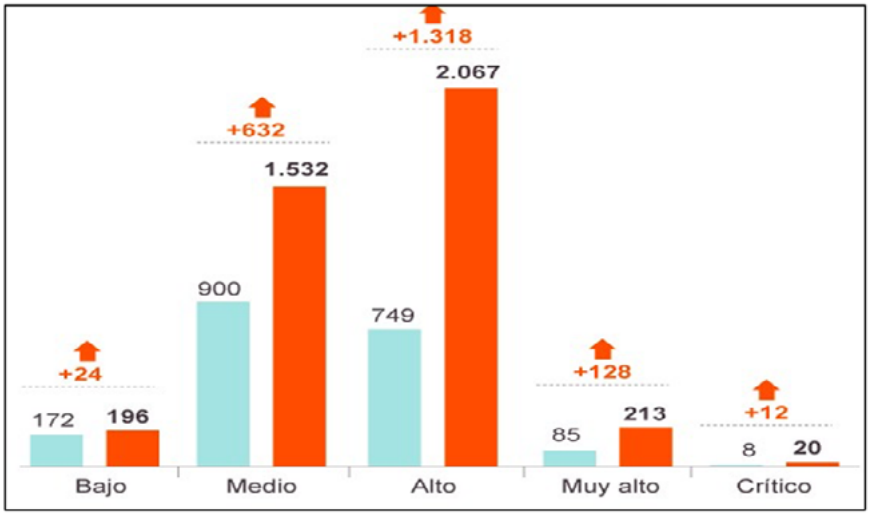
El Plan de Recuperación de Plan de Datos es un plan de emergencia que ha estado en el mercado a nivel mundial y se le atribuye un grado mayor de madurez debido a la cantidad de versiones graduales que ha tenido a lo largo de los años para garantizar una mejor seguridad y un mejor almacenamiento de información, haciéndose cada vez más factible para que las empresas y entidades puedan valerse de ella en caso de que pase alguna contingencia de gran impacto. En la actualidad, son pocas las empresas que utilizan este método para tener un rápido y eficaz manejo de la información, de la actividad y del equipo tecnológico que se desarrolla dentro de las corporaciones. La tecnología surge por primera vez en Europa por lo que debería ser factible que los países europeos sean los primeros que manejen este tipo de método dentro de sus empresas no sólo para un mejor manejo de la información sino también para prevenir una posible amenaza o impacto de una eventualidad futura que puede ocurrir dentro de las distintas áreas laborales, para así garantizar la seguridad y la eficiencia de dicha información.

Sin embargo, España es uno de los países en donde el 32% de las organizaciones no cuentan con un plan de emergencia en caso de desastre para recuperar la información de su infraestructura de

TI que posibilite el trabajo de los sistemas en un plazo no mayor de 24 horas. Se hace notar que España está en una posición mayor que los otros donde el 45% de las organizaciones no presentan un plan de recuperación de datos en caso de que ocurra una contingencia informática; estas cifras manifiestan la preocupación, la insatisfacción y la problemática a la que se enfrentan los profesionales en seguridad cuando hacen propuestas de planes de recuperación de datos ante desastres.

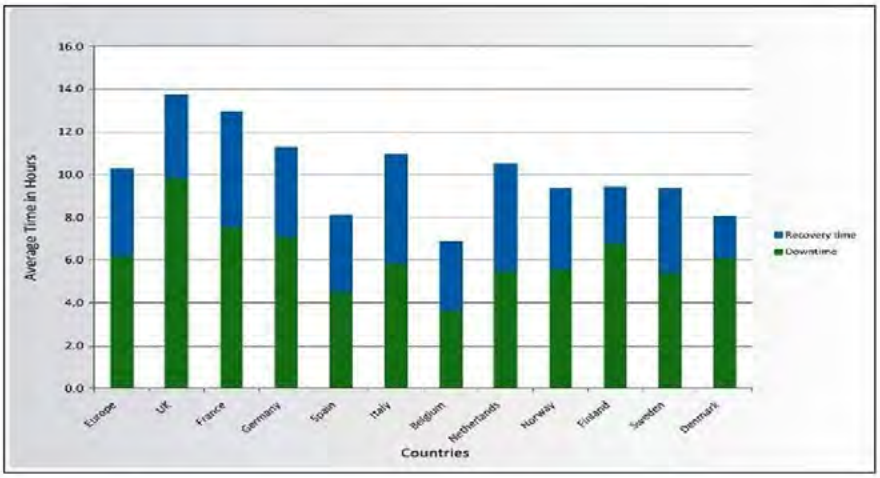
En el Gráfico 1, se muestran los incidentes cibernéticos en el período 2011-2012 donde el gobierno español desarrolló un plan de emergencia. Más adelante, en el Gráfico 2, se muestra el tiempo en que los países de Europa tardan en recuperarse ante un desastre.

Gráfico 1
Incidentes cibernéticos, criticidad de los incidentes 2011-2012



Fuente: Centro Criptológico Nacional/ El País, 2013.

Gráfico 2
Tiempo muerto vs. Tiempo de recuperación en los países de Europa



Fuente: TECNIDA, 2013.

Por otro lado, se puede verificar que Estados Unidos se dio cuenta de esta problemática cuando sucedió el atentado terrorista del 11 de septiembre de 2001; debido a que, a raíz de esto, desaparecieron múltiples compañías que obraban en el World Trade Center por no tener un plan de recuperación de datos. Mientras que, el Wall Street en Nueva York detuvo de inmediato el intercambio de valores lo que origina el cierre de la bolsa durante cinco días, el plazo más largo en la historia financiera desde la Primera Guerra Mundial. Esto ocasionó que Alemania perdiera ese mismo día al final de la tarde un 10% de su valor, que Tokio bajara su índice Nikkei y que las compañías de seguros tuvieran pérdidas de un valor de 42 millones de euros.

Entre tanto, en Sudamérica las entidades gubernamentales obligan a las organizaciones a tener unos planes de emergencia para la recuperación ante cualquier contingencia, como es el caso de Chile, en donde la Superintendencia de Bancos exigen a las entidades financieras a tener un plan de emergencia para recuperar sus sistemas ante cualquier contingencia en el menor plazo de tiempo y exige que este plan sea reestructurado al menos una vez al año para su mejor funcionamiento.

II. Consideraciones sobre el plan de recuperación de datos en organizaciones de Perú

Mediante el sistema de Gestión de Continuidad del Negocio (ISO 22301), se establecerá un Plan de Recuperación de Datos en caso de que la infraestructura tecnológica se interrumpa para lograr contemplar la reanudación de las operaciones en un tiempo estimado y, por ende, generar la confianza en los clientes. La mejor manera de validar que el diseño y establecimiento de controles de seguridad que se propone permitan la recuperación de información en caso de cualquier incidente al considerar lo siguiente:

– Listar los requerimientos legales y normativos

En este caso, se tomarán como base la ISO 22301, la Normativa Técnica Peruana (NTP-ISO 17799:2007) y la Ley de Protección de Datos Personales de Perú n.º 29733.

–Definir los alcances del Sistema de Gestión de Continuidad del Negocio

Se tomará en cuenta un modelo de Recuperación de Datos y Planes de Contingencia definiendo el límite del sistema, es decir, qué módulos se contemplan para la restauración de la operatividad del negocio.

– Establecer las distintas políticas de la Continuidad del Negocio

Se definirán aquellos lineamientos y/o estándares que deben aplicarse en caso de ocurrir un desastre natural o inducido.

– Establecer los objetivos específicos y generales de la Continuidad del Negocio.

Los objetivos forman parte del proyecto y quedan resumidos en el diseño y establecimiento de controles de seguridad para la recuperación de datos en caso de desastre al usar el protocolo IPv6.

– Evidenciar las competencias del personal

Debe realizarse, al mismo tiempo con el área de Recursos Humanos, un estudio del nivel de conocimiento y competitividad del personal con el que cuenta la empresa para definir los roles específicos que deben cumplir las personas asignadas en caso de ocurrir una interrupción del sistema.

– Registrar la comunicación entre todas las partes interesadas

Deben registrarse como una forma de auditoría interna todas las comunicaciones en caso de una contingencia, así como se deben registrar los incidentes ocurridos y las acciones tomadas para resolverlas en forma secuencial.

– Analizar el impacto en el negocio

Hacer el estudio del impacto es un valor agregado del plan de recuperación de datos, medir el impacto en las operaciones y sostenibilidad del negocio permitirá identificar todas las variables y elementos que intermedian en el plan de recuperación de datos.

– Evaluación de los riesgos al considerar su perfil

Mitigar los riesgos implica evaluarlos con cuidado; identificar las vulnerabilidades actuales y amenazas latentes nos permitirá definir de manera adecuada un perfil del riesgo, es decir, que se debe controlar ante todo en caso de ocurrir una catástrofe natural o inducida.

– Estructuras planes de contingencia a incidentes

Los planes de contingencia permiten la medición de la eficiencia de los controles de seguridad establecidos.

– Establecer procedimientos de recuperación

Con los procedimientos y políticas de seguridad, el diseño basado en el protocolo IPv6 para la réplica y restauración de la base de datos per-

mite esclarecer las configuraciones pertinentes de los equipos de red perimetrales como también de los servidores de base de datos, dominios, archivos y correos.

– Evaluar siempre las soluciones de las acciones preventivas, de la supervisión y la medición

La mejora continua forma parte de cualquier ISO, como tal en el proyecto basado en la ISO 22.301 mediante gráficos analíticos y estadísticos se evalúan las acciones tomadas por cada control de seguridad.

III. Informática Empresarial

Para que una empresa esté por completo estructurada y tenga una estabilidad en los sistemas tecnológicos, es necesario que cuente con la participación de la Informática Empresarial, debido a que permite que la misma tenga una estructura y una base de datos que agilice la función de los equipos, de los sistemas y de las aplicaciones tecnológicas que son utilizadas por los trabajadores dentro de la organización. Así mismo, permite la organización, la operatividad y el mantenimiento de toda la infraestructura de TI (*hardware*, *software*, etc.). Por otro lado, la Informática Empresarial es la encargada de la producción eficiente y eficaz de todas las actividades que son realizadas en la empresa con el fin de generarle negocio y valor a la misma; al mismo tiempo que administra las copias de seguridad y la recuperación de datos de toda la empresa en caso de que haya una incidencia que genere un impacto dentro de las actividades que son realizadas a diario por los trabajadores en dicha empresa. De esta manera, en los momentos actuales se puede evidenciar el aumento de la necesidad del plan de recuperación en caso de desastre dentro de las organizaciones al demostrar que la Informática Empresarial es un factor importante y decisivo para todas aquellas organizaciones que se nutren de la tecnología para realizar su trabajo.

IV. Protocolo IPv4

Antes de adentrarse justo en el protocolo IPv4, es necesario definir IP, el cual consiste en ser ante todo una dirección informática, es decir,

cuando un individuo se conecta a internet, el dispositivo electrónico con el que se conecta es re-direccionado con una dirección IP, así como también cada página web tiene una dirección IP. Cuando nace el Internet, nace la dirección IPv4 (Protocolo de Internet Versión 4), que luego es desplazado por el IPv6 (Protocolo de Internet Versión 6) cuando el Internet aumenta sus espacios de direcciones y tamaños. El IPv4 se caracteriza por tener un espacio limitado de 4.3 mil millones de direcciones; es un número de 32 *bits* estructurado en 4 octetos (8 *bits*) en un clave decimal que son separados por puntos.

V. Protocolo IPv6

Los Protocolos de Internet Versión 6 (IPv6) se crean a medida que el Internet se actualiza y, por tanto, aumenta su capacidad de direcciones y tamaños. Estos protocolos se caracterizan por tener direcciones de 128 *bits*, por lo que se define como una dirección que posee un espacio más extenso que el IPv4 y, por tanto, no es necesario tener clave decimal. Está estructurado por ocho secciones de 16 bits que están separadas por dos puntos. Es por esto que, en la actualidad, se utiliza el protocolo IPv6 para las propuestas de planes de recuperación de datos, pues abarcan mucha más información que el IPv4 y están más actualizadas.

VI. Relación entre el protocolo IPv4 y el protocolo IPv6

En la actualidad, la Informática Empresarial en todos los países diseñan los controles de seguridad al usar el protocolo IPv6 debido a que la utilización de este protocolo conlleva un estudio de *hardware* minucioso porque los proveedores de internet ya no cuentan con las direcciones IPv4 públicas. Es por esto que, en el futuro, cada dispositivo electrónico deberá contar con un direccionamiento de red que le permita estar en conectividad constante en la nube a través de la utilización del IPv6. Es por esto que se presenta en la Tabla 1 los rasgos y las diferencias del protocolo IPv4 y el protocolo IPv6.

Tabla 1
Diferencia entre IPv4 vs IPv6

IPv4		IPv6
Direcciones de origen y destino son de 32 bits o 4 bytes		Direcciones de origen y destino son 128 *bits* o 16byte
Total de espacio IPv4: 4,294,967,296 direcciones	Total de espacio IPv6: 340,282 ,366,920,938,463,463,374,607 ,431,768, 211,456 direcciones.	
Cabecera incluye la suma de comprobación		Cabecera no involucra la suma de comprobación
Cabecera incluye opciones		Todos los datos opcionales se trasladaron a las cabeceras de extensión IPv6
Direcciones de difusión se emplean para enviar paquetes a todos los nodos de una subred		No existen direcciones de difusión alcanza su lugar de enlace local de todos los nodos
Configuración manual o DHCP basado en IP		Sin necesidad de configuración manual o DHCP. Los nodos son capaces de auto-configuración

Fuente: CISCO, 2008.

VII. Fundamentos teóricos sobre los sistemas de recuperación de datos ante un desastre

En primer lugar, el investigador Alberto Alexander Servat presenta su artículo: "Nuevo Estándar Internacional en Continuidad del Negocio ISO 22301:2012"[1]. Aquí su objetivo fue determinar los requerimientos para un enfoque de sistemas de gestión para una Continuidad del Negocio en base a prácticas adecuadas para facilitar su uso en las or-

1 Alberto Alexander Servat. *Nuevo Estándar Internacional en Continuidad del Negocio ISO 22301:2012*, Santo Domingo, República Dominicana, Torre Piantini, 2012, disponible en [http://www.gestion.com.do/pdf/018/018-nuevo-estandar-internacional.pdf].

ganizaciones pequeñas, medianas y grandes que obran en los sectores industriales, comerciales, públicos y de beneficencia. Aplica en su metodología el ciclo Plan-Do-Check-Act –PDCA– para la estructuración, el establecimiento, la aplicación, la revisión, el mantenimiento y la mejora constante de su eficiencia, lo que lleva a la conclusión de que, con las nuevas reglas de los mercados internacionales, las organizaciones tienen la obligación de demostrar que son proveedores seguros y confiables; que, ante la presencia de cualquier incidencia alarmante, si la organización tiene un SGCN implementado puede afrontar la contingencia, reanudar sus actividades y seguir ofreciendo sus servicios y/o productos dentro de un plazo estimado.

También está A. ROJAS, con su artículo: "Continuidad de negocio: Estrategias de Respaldo y Recuperación ante desastres"[2] en donde el objetivo fue tener una estrategia básica de respaldo y de recuperación que consta de establecer un ranking de su información más sensible a su negocio e identificar dónde se halla. Su metodología es mantener un plano lógico de acceso a dicha información con el fin de conocer quiénes la utilizan y cómo se vería afectado el negocio en ausencia de la información. Se llega a la conclusión que debe haber mejores prácticas de gestión de la Continuidad del Negocio y la necesidad de revisar todo el tiempo el proceso con el propósito de mejorarlo.

Por otro lado, GENARO MÉNDEZ JIMÉNEZ en su tesis "Plan de Recuperación de desastres del Sistema SAP"[3], plantea que hay una falla en el servidor aplicativo en un laboratorio farmacéutico y establece un Plan de Continuidad del Negocio al tomar en cuenta el Punto de Recuperación de la Información –RPO– y el tiempo en el que debe recuperarse la Información –RTO–. Su metodología se basó en los índices, análisis y diseño que ostenta Symantec (Corporación Internaciones que desarrolla y comercializa *software* en particular en el dominio de la Seguridad Informática). El escenario considera las fallas de la infraestructura

---

2 A. ROJAS. *Continuidad de negocio: Estrategias de Respaldo Recuperación ante Desastres*, diciembre de 2011.

3 GENARO MÉNDEZ JIMÉNEZ. *Plan de Recuperación de Desastres del Sistema SAP Considerando Falla en el Servidor Aplicativo de un Laboratorio Farmacéutico*, México, D. F., 2012, disponible en [http://132.248.52.100:8080/xmlui/bitstream/handle/132.248.52.100/2881/Tesis.pdf?sequence=1].

del sistema SAP como el modo de recuperación de la operatividad de la empresa mediante servidores espejo, ubicado en oficinas alternas; como parte de la solución elabora la documentación pertinente a través de un caso práctico donde muestra los resultados del DRP, así como el entrenamiento, la actualización y el soporte al personal. Por otro lado, al darse cuenta que SAP es el principal sistema de información del Laboratorio Farmacéutico estudiado, se genera repercusiones graves a la organización lo que demuestra que la aplicación oportuna de un Plan de Continuidad del Negocio tomará unas medidas preventivas para que el área de TI garantice la restauración del servicio en base a un plan de recuperación de datos ante cualquier desastre; la prioridad es asegurar la disponibilidad del servicio para que los procedimientos y los controles establecidos sean con éxito desplegados por el personal involucrado.

Mientras que, ALEXANDER SERVAT en su artículo "Gestión del Riesgo en el Business Continuity Planning"[4], tuvo como objetivo identificar todos aquellos factores que perjudican a los activos de las funciones empresariales. Su metodología consistió en calcular a cada amenaza identificada, la posibilidad de ocurrencia y el impacto que puede ocasionar en la empresa a nivel económico. Por lo tanto, es en esta etapa donde la empresa debe tomar decisiones sobre las alternativas de tratamiento del riesgo, disipar qué amenazas se afrontarán con controles, cuáles admitirán, y cuáles se traspasarán; permitiendo concluir que es importante poder identificar varios escenarios de amenazas que puedan perjudicar las funciones y actividades de la empresa.

Por otro parte, los profesionales informáticos EDUARDO CASARERO, ALEJANDRO CLEMENTE y SANTIAGO RUIZ en su documento "IPv6"[5], describen las principales características y ventajas tecnológicas del protocolo IPv6, así como plantean los métodos de transición desde el IPv4 al mostrar el impacto de este protocolo en una organización.

---

4 ALBERTO ALEXANDER SERVAT. *Gestión del Riesgo en el Business Continuity Planning*, Lima, 2006, disponible en [https://docplayer.es/2838466-Gestion-del-riesgo-en-el-business-continuity-planning.html#download_tab_content].

5 EDUARDO CASARERO, ALEJANDRO CLEMENTE y SANTIAGO RUIZ. *IPV6*, Buenos Aires, Universidad Argentina de la Empresa, 2011, disponible en [https://docplayer.es/2097861-Ipv6-casarero-eduardo-clemente-alejandro-ruiz-santiago-universidad-argentina-de-la-empresa.html].

Por consiguiente, este trabajo informático estructura la transición de IPv4 a IPv6 y analiza el impacto tecnológico en la empresa. Hoy en día, los motores de búsqueda ofrecen información acerca del tema, sin embargo, aún no existen tendencias claras en cuanto a cómo resolver algunos problemas de la transición; por ende, la Organización Internacional "Internet Engineering Task Force" –IETF– cuenta con un equipo de trabajo IPv6 que son responsables de la especificación y caracterización del Protocolo de Internet Versión 6. Es imperativo afirmar que la transición a IPv6 se da poco a poco por lo que Cisco Systems estima que millones de ingenieros deben ser capacitados en este protocolo debido al inevitable decaimiento de las direcciones IPv4 en un futuro. La concientización de los usuarios, de los profesionales en TI y los proveedores de internet respecto a las ventajas tecnológicas que tiene el protocolo IPv6 debe ser fundamental para acelerar su uso que, desde inicio de los noventa, viene desarrollándose como una solución frente a la saturación de direcciones IPv4. También, se menciona que el IPv5 fue el inicio de este proyecto que luego implantó las nuevas tendencias y constituyó la plataforma inicial para la evolución de IPv6. A pesar de su avance, aún hay muchos puntos qué resolver como el hecho de cómo se debe realizar una transición ordenada, por lo que se necesita el apoyo de las universidades y de los centros tecnológicos al incorporar el protocolo IPv6 en sus síntesis curriculares para proponer mejoras en las redes de datos y telefonía de las empresas.

Del mismo modo, Cisco en su artículo "Ipv6 Addressing White Paper"[6], dispone que la solución frente a la saturación de direcciones IPv4 es la migración a IPv6 a razón de su amplio espacio de direcciones (340 undecilliones aprox.), así como las técnicas y/o métodos para su despliegue y transición transparente. En la actualidad, la Autoridad de Números Asignados en Internet –IANA– es la responsable de designar las direcciones IP a los Registros Regionales de Internet, ellos a su vez asignan bloques de direcciones a los proveedores de servicio de Internet; cada proveedor se encarga de distribuir las direcciones a sus clientes respectivos.

---

6 CISCO. *IPV6 Addressing White Paper*, San Jose CA, EE. UU., 2008, disponible en [https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/IPv6_WP.pdf].

El Gobierno Regional de Ica en el plan "Regional de Prevención y Atención de desastres 2009-2019"[7] propone los mecanismos de prevención para salvaguardar a la población ante desastres, al otorgar el soporte necesario y la ayuda oportuna que permitirá una eficaz rehabilitación. A su vez plantea la estrategia y las medidas técnicas y legales que se deben considerar para la operatividad y el funcionamiento del Plan Regional. Este estudio establece las incidencias naturales y tecnológicas en potencia latentes y, a raíz de ello, establece las políticas y los procedimientos que deben seguirse en caso de ocurrir un desastre de cualquier índole; en consecuencia, plantea la organización y ejecución de acciones preventivas como prioridad frente a las correctivas. En efecto, el estudio se centra en los escenarios de riesgo que enfoca los desastres naturales y antrópicos ocurridos en el pasado lo que deriva en el análisis de las amenazas y vulnerabilidades sobre la dinámica y frecuencia de estos fenómenos. Al usar como referencia el terremoto del 15 de agosto del 2001, ocurrido en el departamento de Ica, provincia de Pisco; se considera que Perú se encuentra en el cinturón sísmico del continente donde la probabilidad de que ocurran movimientos sísmicos de gran magnitud es alta. Sin embargo, los sismos no son los únicos desastres a considerar, también se dan con frecuencia inundaciones, siendo latentes los tsunamis como parte de los desastres naturales; y, respecto a los antrópicos, se dan con recurrencia los incendios. Por último, el desenlace de este plan lleva a gestionar con eficacia las políticas de prevención y de medidas correctivas en caso de desastre promoviendo el desarrollo y la participación integral de las autoridades y la población en general, para controlar el impacto teniendo como prioridad salvaguardar las vidas humanas en base a los datos estadísticos que permite inferir y analizar la ocurrencia de los desastres, así como también conocer las medidas preventivas y de atención que se deben considerar en caso de catástrofe.

---

7 Gobierno Regional de Ica. *Plan Regional de Prevención y Atención de Desastres Región Ica 2009-2019*, Ica, 2009, disponible en [https://www.paho.org/per/index.php?option=com_docman&view=download&alias=219-plan-regional-prevencion-atencion-desastres-region-ica-2009-2019-9&category_slug=planes-procedimientos-protocolos-945&Itemid=1031].

Capítulo segundo
Epistemología de los controles de seguridad para la recuperación de datos en caso de desastre

I. Normativas ISO 22301:2012

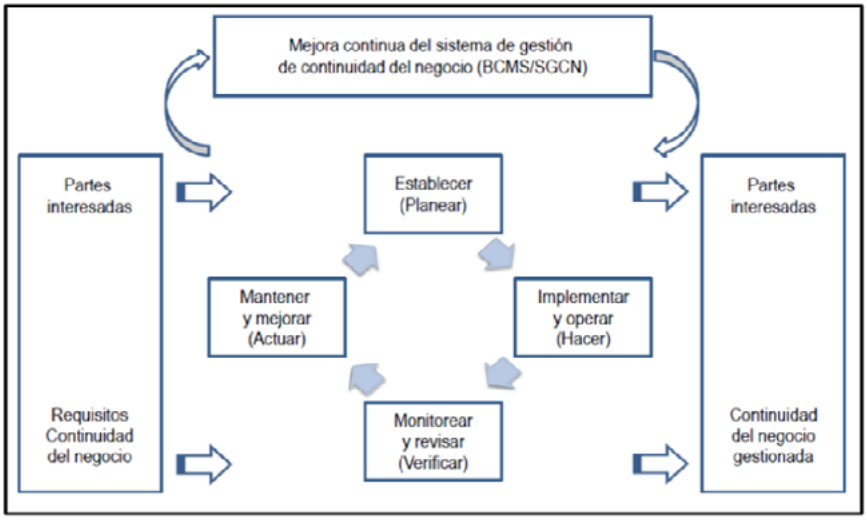
La norma ISO 22301 es la primera norma internacional para gestionar la progresividad de negocio –GCN– y ha sido desarrollada para brindar ayuda a las empresas u entidades, a disminuir el riesgo de este tipo de interrupciones conocida como sistemas de gestión de la continuidad de negocio –SGCN– esta norma sustituirá la norma actual británica BS25999. La misma, provee una base de entendimiento, desarrollo e implantación de continuidad de negocio dentro de su organización y le ofrece confiabilidad de negocio a negocio y de negocio a cliente. Se emplea para darle seguridad a las partes interesadas clave de que su organización está por completo dispuesta y que posee la capacidad de dar cumplimiento a los requerimientos internos, de normalización y del cliente.

En este sentido, la norma suministra a las estructuras organizativas un marco que garantiza que ellos pueden prolongar sus labores durante las situaciones más arduas e imprevistas, dándoles protección a sus trabajadores, al sostener su reputación y facilitar las posibilidades de laborar y comercializar a pesar de cualquier circunstancia.

A. Ciclo PDCA

La norma ISO 22301 expone, de manera específica, requerimientos para planear, estipular, instaurar, manipular, monitorear, examinar, sostener y optimizar de forma continua un sistema de gestión documentado para prepararse, dar respuesta y alcanzar recuperaciones de eventualidades que generan paralizaciones, cada vez que estos suceden.

Figura 1
Ciclo PDCA ISO 22301



Fuente: NORMA ISO 22301:2012.

Tabla 2
Descripción de los elementos del PDCA

Plan (establecer)	Establecer políticas, objetivos, metas, controles, procesos y procedimientos relacionados con la mejora de continuidad de negocio con el propósito de alcanzar resultados que se alinean con las políticas y los objetivos generales de la estructura organizativa.
DO (implementar y operar)	Implementar y operar las políticas, los controles, procesos y procedimientos.
Check (monitor y revisión)	Seguimiento y evaluación de desempeño, informará de los resultados a la gerencia para su revisión y autorizar las acciones de remediación y mejoramiento.
ACT (mantener y mejorar)	Mantener y mejorar la SGCN al adoptar las medidas correctivas, en base a los resultados del examen de la gestión y la revalorización del ámbito de aplicación del BCMS y continuidad de negocio y objetivos.

Fuente: elaboración propia.

B. Alcance de ISO 22301

Un sistema de gestión de continuidad de negocio alineado con las normas ISO 22301 es apropiado para todo tipo de estructura organizativa, sin importar tamaños y rubros, desde el sector público al privado. La política es en particular relevante en aquellas empresas que laboran en contextos de elevados riesgos, donde la destreza de llevar a cabo tareas laborales de forma progresiva y permanente es fundamental para los negocios, clientes e interesados, esto brindará los siguientes beneficios:

– Desarrollar un análisis de riesgos a fin de establecer las acciones de mitigación que correspondan.

– Planear las operaciones y procesos dirigidos a sostener la operatoria de la organización ante circunstancias de incidencia.

– Recuperar en lapsos de tiempo mínimos y al menor costo posible, la continuidad de las prestaciones de procesos paralizadas por la emergencia.

– Evitar la pérdida de datos.

La norma ISO 22301 permitirá:

– Estipular, implementar, sostener y alcanzar mejoras en su Sistema de Gestión de Continuidad de Negocio.

– Cumplir con los requerimientos de la política de continuidad de negocio.

– Brindar a los interesados la confiabilidad en su conformidad y responsabilidad con las mejores prácticas reconocidas a nivel internacional.

– Obtener la certificación de BSI en su sistema de gestión de continuidad de negocio.

C. Continuidad de Negocio: Estrategia

La gestión de la continuidad no se instaura cuando sucede un desastre, sino que se refiere a todas aquellas tareas que se ejecutan a diario para sostener el servicio y hacer más fácil la recuperación. La norma ISO 22301 fue creada para gestionar de manera correcta el Plan de Continuidad del Negocio en una estructura organizativa.

La gestión de la continuidad del negocio aminorará las posibilidades de que ocurra una eventualidad disruptiva y, en caso de originarse,

la organización tendrá la preparación para dar respuesta de manera apropiada, a los fines de reducir de forma drástica el daño potencial de esa incidencia.

De igual manera, es oportuno mencionar, que gestionar e implantar un SGCN no sólo emerge como réplica al riesgo que presume la interrupción de una organización, sino también, debido a la conciencia que existe sobre el deterioro que padece el perfil de esa organización cuando se hace de conocimiento público su impedimento para dar continuidad de negocio en casos de desastres. Por ello, las organizaciones que gocen de forma garantizada de la Continuidad de Negocio a través del sistema ISO 22301, poseen la ventaja de que el impacto que pueda generar un desastre sea nimio.

El modelo actual presenta exigencias de determinada documentación. La empresa está en la obligación, de acuerdo a su alcance de desplegar los siguientes:

- Lista de requerimientos legales, normativos y de otra índole.
- Alcance del SGCN.
- Política de la continuidad del negocio.
- Objetivos de la continuidad del negocio.
- Demostración de aptitudes del personal.
- Registros comunicativos con los involucrados.
- Estudio del impacto en el negocio.
- Evaluación de riesgos, incluyendo un perfil del riesgo.
- Organización de respuesta a incidencias.
- Planificación de continuidad del negocio.
- Operaciones de recuperación.
- Resultados de gestiones provisorias.
- Resultados de verificación y medición.
- Resultados de la auditoría a nivel interno.
- Resultados de la exploración por parte del director.
- Resultados de gestiones de enmienda.

Tabla 3
Estructura de la continuidad de negocio

Disaster Recovery Plan (drp)	Contingency Plan (cp)	Business Continuity Plan (bcp)
Está enfocado en la recuperación ante un desastre. Por ejemplo, el centro de cómputo de una compañía.	Permite la recuperación de una a más funciones específicas críticas de la empresa. Por ejemplo, el sector de tesorería	Su implementación permite estar prevenido ante desastres de cualquier tipo, que afecte el normal desenvolvimiento en todos sus aspectos y áreas. El bcp incluye al drp

Fuente: norma iso 22301:2012.

D. Plan de Recuperación de Datos

El Disaster Recovery Plan –drp– es la estrategia que se emplea para restituir los servicios de TI posterior al padecimiento de los efectos de un desastre natural. La elevada dependencia en las Tecnologías de Información y telecomunicaciones, ha generado la necesidad de las empresas de implementar medidas preventivas apropiadas, así como con el conocimiento para recuperar la destreza de entregar servicios de TI en el tiempo estipulado, siempre con alineación a las necesidades de los procedimientos de negocio. El drp brinda apoyo a las estructuras organizativas para desarrollar, establecer y mejorar sus planificaciones de recuperación en caso de catástrofe en todas sus fases, esto es, identificar servicios y recursos críticos de TI, comprender los riesgos e impactos por paralizaciones, precisar estrategias y planes de recuperación, dar entrenamiento al personal, ejecutar ejercicios de prueba y mantener actualizados los planes y procesos asociados al plan[8].

La dirección de la organización debe considerar la decisión de comenzar el plan como un proyecto para así dar cumplimiento a los objetivos que se presentan a continuación:

– Estipular la fragilidad a las paralizaciones del servicio relevantes en el centro de datos e instalaciones de negocios y precisar las medidas de prevención que se pueden considerar a los fines de comprimir de forma mínima la posibilidad y el impacto de las paralizaciones.

8 pecb. *iso 22301*, 2012, disponible en [http://pecb.org/iso22301/].

– Identificar y estudiar el costo, servicio, el perfil público y otras secuelas de las interrupciones dilatadas del servicio en el centro de datos y otras instalaciones de la empresa.

– Fijar las necesidades inmediatas, a medio y largo plazo, de recuperación y los recursos requeridos.

– Identificar las opciones y hacer una selección de los métodos más beneficiosos, en aras de proporcionar la funcionalidad de los procedimientos de copia de seguridad y el restablecimiento de un servicio en los lapsos de tiempo adecuados.

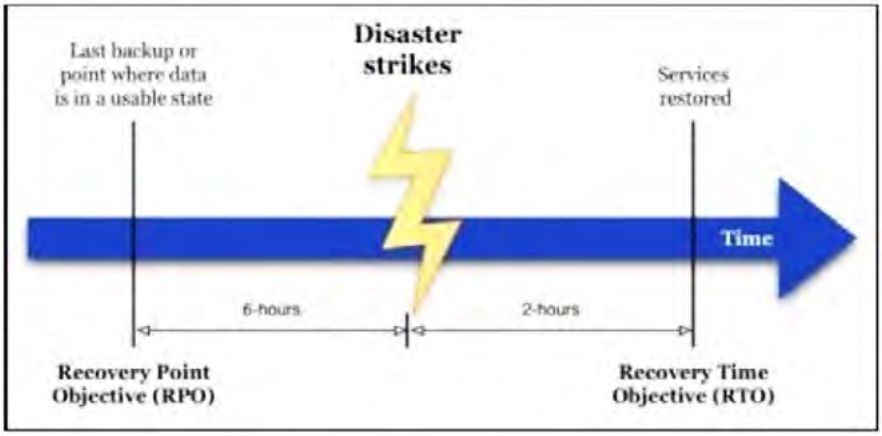
– Desarrollar e implementar procedimientos que se ocupan de las necesidades más urgentes y de largo plazo para el centro de datos y otros servicios de la empresa.

El propósito fundamental de un DRP es comprimir de forma mínima el tiempo de inactividad tecnológica y la pérdida de información con una recuperación metódica luego de una catástrofe. Para disminuir el tiempo de inactividad y la pérdida de información es necesario tomar en consideración lo siguiente:

– Objetivo de Tiempo de Recuperación (RTO, Recovery Time Objective) es el lapso de tiempo en el que el proceso de negocio debe estar restituido, luego de una eventualidad grave, con la finalidad de sortear secuelas inadmisibles procedentes de un rompimiento en la continuidad del negocio. Para reducir el RTO, se necesita que la Infraestructura (tecnológica, logística o física) tenga disponibilidad en el menor tiempo posible, una vez que ha pasado la eventualidad de interrupción.

– Objetivo de Punto de Recuperación (RPO, Recovery Point Objective) hace referencia al volumen de datos en riesgo de pérdida que la estructura organizativa considera admisible para los procedimientos, posterior a una incidencia de gravedad. El RPO se enuncia hacia atrás en el tiempo (en el pasado) desde el momento en que la eventualidad se origina, y puede ser representados en segundos, minutos, horas o días, por esa razón, es la cantidad máxima admisible de pérdida de los datos medidos en el tiempo. Para reducir un RPO se requiere incrementar el sincronismo de réplica de datos.

Figura 2
Diagrama RTO/RPO



Fuente: Macexperts, 2010.

El Plan de Continuidad de Negocio –BCP– posee la particularidad de clasificar los procedimientos de negocio en función de su criticidad y lo que es más relevante: estipular la primacía de recuperación (o su orden secuencial).

La estructura debería poseer los puntos mencionados a continuación:

- Pre-planificación de acciones: plan de trabajo.
- Evaluación de la vulnerabilidad: informes de evaluación de la seguridad.
- Análisis de impacto al negocio.
- Conceptualización pormenorizada de los requerimientos: necesidades de recuperación, contexto de aplicación, objetivos y supuestos.
- Plan de desarrollo: centro de datos, reanudación de unidades de negocio, reglas de recuperación, *backups*, etc.
- Programa de pruebas: estrategias de ensayo, objetivos de pruebas y ejercicios.
- Programa de mantenimiento: operaciones de actualización.
- Prueba inicial e implementación.

Los elementos esenciales para un plan sólido de recuperación ante desastres son:

E. Definición del Plan

Para que un Plan de Recuperación ante Desastres funcione, tiene que envolver a la Gerencia de la organización. Ellos son los garantes de su coordinación y deben asegurar su carácter efectivo. Además, deben proporcionar los recursos suficientes para un progreso eficaz del plan. Todas las áreas de la estructura organizativa tienen participación en la determinación del plan.

F. Establecimiento de Prioridades

La compañía debe realizar un análisis de riesgo y fundar una lista de catástrofes naturales o desastres ocasionados por errores de seres humanos, y clasificarlos de acuerdo a sus posibilidades. Una vez culminada la lista, cada área debe estudiar los potenciales efectos y el impacto concerniente con cada tipo de catástrofe. Esto tendrá utilidad como referente para la identificación de lo que se requiere incluir en el plan. Se fija un orden de recuperación de acuerdo al nivel de relevancia.

G. Selección de estrategias de recuperación

En esta fase se establecen las opciones de más practicidad para proceder en caso de un evento catastrófico. Todos los elementos de la estructura organizativa son estudiados. Las opciones a considerar varían de acuerdo con la función del TI, de igual modo, se examinan los costos asociados.

H. Componentes esenciales

El manuscrito establece los procesos, identifica las fases fundamentales, excluye redundancias, al considerar el mantenimiento y la actualización del plan a medida que el negocio progresa. El plan determina compromisos a diversos equipos / departamentos y electivos.

I. Criterios y procedimientos de prueba del plan

Los planes de recuperación deben ser sometidos a prueba de manera total y absoluta por lo menos una vez al año. La documentación debe presentar de forma específica los procedimientos y la periodicidad con que se ejecutan las pruebas. Los argumentos más relevantes para ejecutar las pruebas del plan son: confirmar la validez y funcionalidad del plan, fijar la compatibilidad de las operaciones e instalaciones, identificar áreas que requieran cambios, brindar entrenamiento a los trabajadores y manifestar la habilidad de la empresa de recuperarse de un desastre.

J. Aprobación final

Posterior a que el plan haya sido probado y corregido, la gerencia deberá emitir su aprobación. Ellos son los garantes de fijar las pólizas, los procesos y compromisos ante cualquier eventualidad.

II. Normativas iso 27001:2013

A. Sistema de Gestión de la Seguridad de la Información

Las Tecnologías de la Información poseen un crecimiento exponencial, han convertido la forma de hacer negocios y el desempeño de las estructuras organizativas. La información representa un activo esencial, que requiere protección, para que las firmas puedan subsistir y competir. El resguardo de la confidencialidad, disponibilidad y la integridad de los datos en las organizaciones, debe ser una inquietud estratégica. Los activos de información están supeditados de manera continua, a una sucesión de amenazas que intentan vilipendiar las vulnerabilidades empresariales. El sgsi es un instrumento muy útil y de mucha relevancia en la gestión de las estructuras organizativas. Aunado a la conceptualización central sobre el que se cimenta la norma iso 27001.

Debido a que la información es uno de los activos de más valía de toda empresa, necesita junto a los procesos y sistemas que la operan, ser resguardados de manera conveniente, de cara a amenazas que pue-

dan poner en peligro la continuidad de los niveles de competitividad, rentabilidad y conformidad legal ineludibles para lograr los propósitos de la organización.

En este sentido, los sistemas de información están supeditados a riesgos e inseguridades, tanto al interior de la propia organización como riesgos externos. A los riesgos físicos (accesos no autorizados a la información, desastres naturales –fuego, inundaciones, terremotos, vandalismo, etc.–) se debe agregar los riesgos lógicos (virus, ataques de denegación de servicio, etc.). Para ello se vuelve indispensable conocer y enfrentar de forma ordenada, los riesgos a los que está expuesta la información, y por medio de la cooperación activa de toda la estructura organizativa, vislumbrar algunas operaciones apropiadas y proyectar e implantar controles de seguridad que tengan como base una evaluación de riesgos y en una medición de la validez de los mismos.

El Sistema de Gestión de la Seguridad de la Información –SGSI– en las organizaciones permite fijar estas políticas, procedimientos y controles de acuerdo a los objetivos de negocio de la empresa, con el propósito de sostener siempre el riesgo por debajo del grado que pueda asumir por la propia organización[9].

La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Estos tres términos constituyen la base sobre la que se cimienta la seguridad de la información:

– Confidencialidad: la información no debe estar disponible ni se revela a personas, instituciones o procesos no autorizados.

– Integridad: sostenimiento de la exactitud y completitud de la información y sus métodos de proceso.

– Disponibilidad: acceso y uso de la información y los sistemas de tratamiento de la misma por parte de sujetos, instituciones o procesos autorizados cuando lo necesiten.

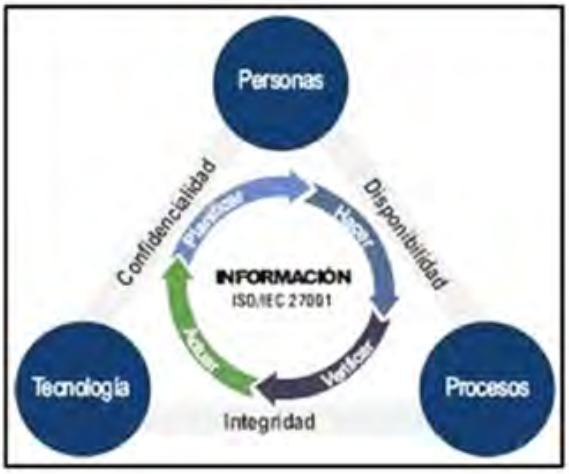
Para certificar que la seguridad de la información es gestionada de forma correcta, se debe emplear un proceso sistemático, documentado

---

9 ICONTEC. *Norma técnica colombiana*, Colombia, ISO, 2013, disponible en [https://colaboracion.dnp.gov.co/CDT/Normograma/NTC-ISO%2030300%20de%202013.pdf].

y conocido por toda la estructura organizativa, desde una perspectiva de riesgo empresarial. Este proceso es el que constituye un SGSI, tal como se muestra en la Figura 3.

Figura 3
Ciclo SGSI



Fuente: Norma ISO 27001:2013.

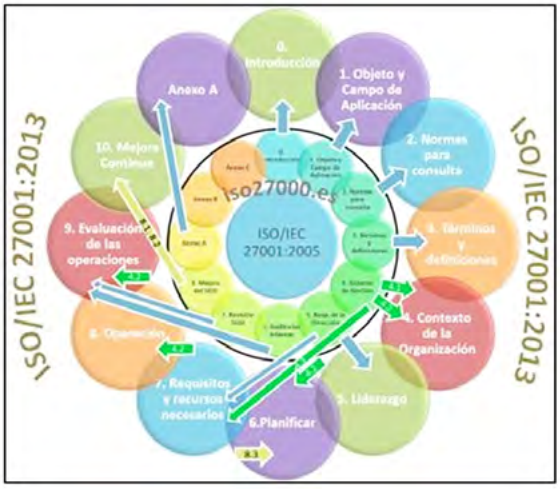
B. Estándares de Gestión

La nueva Norma ISO 27001:2013 tiene la característica de ajustar los requerimientos relativos a la gestión documental a todas las normas de gestión, brinda una elevada flexibilidad en lo concerniente a la selección de métodos de trabajo de análisis de riesgos o de mejora continua. Se destaca un nuevo dominio que se crea sobre "Relaciones con el Proveedor" debido a la evolución a la nube o *Cloud Computing*.

La perspectiva del análisis del riesgo en la fase de planificación y operación, a partir de ahora para identificar los riesgos no se requiere la identificación de los activos, las amenazas y sus vulnerabilidades. Sino que se inicia del análisis de riesgos para fijar los controles fundamentales y compararlos para que no se olvide ninguno aplicable[10].

10 Ibíd.

Figura 4
Modificaciones de versión entre 2005 y 2013



Fuente: Norma ISO 27001:2013.

Trabaja en función a ocho principios de gestión:

1. Orientación al cliente.
2. Liderazgo.
3. Participación del personal.
4. Enfoque de procesos.
5. Enfoque de sistemas de gestión.
6. Mejora continua.
7. Enfoque de mejora continua.
   Relación en conjunto beneficiosa con el proveedor.

La normatividad integra las siguientes normas y términos de uso:

– ISO 30301:2011, Información y documentación - Sistemas de gestión de documentos - Requisitos (armonizado con el anexo SL).

– ISO 22301:2012, La seguridad societaria - Los sistemas de gestión de continuidad de negocio - Requisitos (armonizado con el anexo SL).

– ISO 20121:2012, sistemas de gestión de la sostenibilidad de eventos - Requisitos con orientación para su uso (armonizado con el anexo SL).

– ISO 27001:2013, sistemas de gestión de la seguridad de la información.

Figura 5
Variantes de las cláusulas de la versión 2013 y 2015

Fuente: NORMA ISO 27001:2013.

En la Tabla 4 se hace una descripción de las ventajas y desventajas de la versión 2013.

Tabla 4
Ventajas y desventajas ISO 27001:2013

VENTAJAS	DESVENTAJAS
Facilita la integración de los sistemas de gestión, debido a que es una estructura de elevado nivel, donde los términos y definiciones permiten implementar.	Es una abstracción y es un nivel alto, no es tan detallado.
Todas las definiciones vienen del estándar ISO 27000 y las inconsistencias se han removido.	Los requisitos son un tanto más difíciles para interpretar, debido a los nuevos conceptos.
Los riesgos en la seguridad de la información en su conjunto deben ser abordados.	No se menciona el enfoque PDCA.
Los documentos requeridos están visiblemente estipulados, hace referencia al tamaño y complejidad.	No se menciona las políticas del SGSI.
Menciona que las acciones preventivas no van.	No hay una descripción detallada de la identificación del riesgo.

Fuente: elaboración propia.

C. Marco Legal

Es una de las normas de sistema de gestión de la seguridad de la información de más veloz crecimiento empleada en todo el orbe. La norma es utilizada para certificaciones de tercera parte acreditadas y cuenta con al menos 17.500 certificados emitidos en 100 naciones con una tendencia progresiva de crecimiento de dos dígitos año tras año. Su uso posee el respaldo del Código de Buenas Prácticas ISO 27002. Ambas fueron desarrolladas a través del consenso de la comunidad internacional con más de 47 organismos nacionales de normalización[11]. Las organizaciones se favorecen con la normatividad:

- Incrementa la reputación de los negocios que han implementado la norma.
- Protege a las organizaciones a través de la identificación de riesgos y estipula controles para gestionarlos o reducirlos.
- Ayuda a los grupos de interés y aumenta la confianza del cliente, teniendo sus datos protegidos.
- Aumenta las oportunidades de acceso a licitaciones mediante la demostración de cumplimiento y obteniendo un estatus como proveedor preferido.

Se ha modificado para adaptarse a la nueva estructura de alto nivel utilizado en todas las normas de Sistemas de Gestión, lo que simplifica su integración con otros sistemas de gestión e incorpora la evolución del panorama tecnológico desde 2006 hasta 2014.

III. Normativas ISO 31000:2009

El objetivo fundamental de la norma ISO 31000:2009 es ayudar a las empresas de todo tipo y/o tamaño a gestionar de forma efectiva el riesgo. Esta norma determina unos principios que deben ser satisfechos para que se haga una gestión eficaz del riesgo. Además, recomienda que las empresas elaboren, desarrollen, apliquen y mejoren de manera

11 Ibíd.

continua una estructura de soporte (*framework*) o un marco de trabajo que tenga como objetivo integrar el proceso de gestión de riesgos en un gobierno corporativo de planificación, organización y estrategia, procesos de información, valores, políticas y cultura[12].

A. Alcance de ISO 31000:2009

Esta norma no es específica a algún sector o industria por lo que puede ser utilizada en cualquier entidad. Por otra parte, se puede implementar a cualquier tipo de riesgo, no importa su naturaleza, origen o causa, sólo que sus consecuencias sean tanto positivas como negativas para la empresa. Por otro parte, tiene un enfoque estructurado en tres factores claves para una gestión de riesgos efectiva: los principios, el marco de trabajo (*framework*) y el proceso de gestión del riesgo.

Esta norma determina aquellas directrices y/o principios de carácter genérico sobre la gestión del riesgo; y para que tenga una mayor eficacia, se deben considerar estos principios:

1. Crea valor.
2. Se integra a los procesos de la empresa.
3. Tiene participación en la toma de decisiones.
4. Maneja la incertidumbre de manera explícita.
5. Es adecuada, sistemática y estructurada.
6. Su base es la mejor información disponible.
7. Está estructurada a medida.
8. Toma en cuenta los factores culturales y humanos.
9. Es inclusiva y transparente.
10. Es interactiva, dinámica y sensible al cambio.
11. Permite la mejora continua de la empresa.

B. Marco de Trabajo

El objetivo de esta estructura de soporte es integrar el proceso de gestión de riesgos al gobierno corporativo reforzando la importancia de las deci-

12 ACT. *ACT Government.*, 2014, disponible en [https://www.legislation.act.gov.au/a/2014-24/].

siones estratégicas de alto nivel en relación a la seguridad de la información. La norma ISO 31000 sugiere el desarrollo, aplicación y mejora continua de un marco de referencia cuya finalidad sea la integridad del proceso de la gestión de riesgo en el gobierno, estrategia, planificación, informes de los procesos, valores, políticas y cultura de toda la empresa[13]. Se puede observar en la Figura 6 el marco de trabajo mediante *framework*.

Figura 6
Marco de trabajo

Fuente: Norma ISO 31000:2009.

C. Ciclo PDCA

La Norma ISO 31000 determina unos mandatos que deben ser cumplidos por la gerencia para asegurar la efectividad de la gestión de riesgos, por lo que se requiere un gran compromiso y una planificación rigurosa y estratégica de la gerencia. Dichos mandatos conforman estos puntos:

- Validar la política de gestión de riesgos.

13 Ibíd.

- Establecer los indicadores de desempeño alineados con los de la empresa.
- Consolidar la estructura de los objetivos de la gestión de riesgos con las estrategias y objetivos de la empresa.
- Garantizar las conformidades legales y regulatorias.
- Establecer las responsabilidades de acuerdo a los diferentes niveles de la empresa.
- Verificar la disposición de los recursos necesarios para la gestión de riesgos.
- Informar a todas las partes interesadas sobre los beneficios de la gestión de riesgos.
- Comprobar que se mantenga un adecuado marco de trabajo para la gestión.

Por otra parte, las cuatro fases del ciclo PDCA aluden a:

1. El diseño de un marco de trabajo para la gestión de riesgo, que incluyen estos puntos: interpretación de la empresa y su contexto interno y externo, política de gestión de riesgos, fusión con los procesos de la empresa, rendición de cuentas, recursos y establecimientos de las comunicaciones internas y externas, y los mecanismos de informes.
2. Implementación del marco de referencia de riesgos en base a la aplicación del marco de trabajo y del proceso para la gestión de riesgos.
3. Revisión y observación de la efectividad del marco de trabajo, establecimiento de las medidas de desempeño y la observación periódica de los avances, desviaciones e informes.
4. Las decisiones que se toman para la mejora continua del marco de trabajo y la cultura correspondiente.

D. Proceso de gestión de riesgos

El proceso está estructurado en tres etapas:

– Establecimiento del contexto

La verdadera base de la norma es determinar el contexto interno y externo en el que opera la empresa que busca alcanzar sus propósitos, así como determinar el proceso para la gestión de riesgos y definir los criterios de evaluación de los mismos.

– Valuación de riesgos

Constituida paso a paso por la Identificación, Análisis y Evaluación de riesgos.

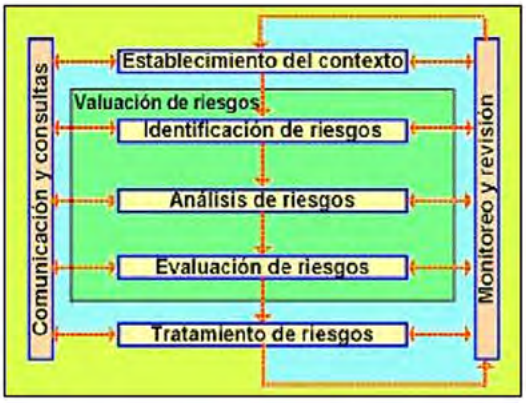
– Tratamiento de los riesgos

Al seleccionar las opciones de tratamiento de los riesgos, la norma establece unas opciones aplicables de manera individual o concurrente en el tratamiento, las cuales son:

a) Impedir el riesgo al decidir no comenzar o continuar con los hechos que pueden originarlo.
b) Incrementar o reconocer el riesgo para concretar una oportunidad.
c) Trasladar la fuente de riesgo.
d) Modificar la probabilidad.
e) Modificar las consecuencias e impactos.
f) Informar a los terceros sobre el riesgo (incluye contratos y financiamientos del riesgo).
g) Retener el riesgo por decisión propia.

A la postre, el proceso de gestión de riesgos se cierra con la interrelación de las etapas mencionadas con la Comunicación y Consultas, por un lado, y con el Monitoreo y Revisión por el otro, tal como se observa en la Figura 7.

Figura 7
Proceso ISO 31000

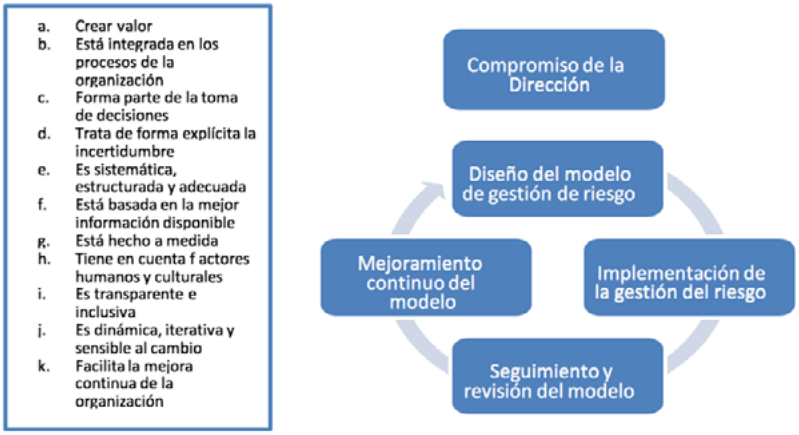


Fuente: Norma ISO 31000:2009.

– Relación de los procesos

En las Figuras 8 y 9 se resume la relación que se establece entre los principios de gestión, el marco de referencia y el proceso de gestión del riesgo desarrollado en la norma.

Figura 8
Integración de Procesos Parte 01



Fuente: Norma ISO 31000:2009.

Figura 9
Integración de Procesos Parte 02

Fuente: Norma ISO 31000:2009.

E. Beneficios que trae la Norma ISO 31000:2009 a las empresas

- Aumento de probabilidades de logro de objetivos.
- Fomentar la gestión proactiva.
- Conciencia de la necesidad de identificación y el manejo del riesgo en toda la empresa.
- Mejora de identificación de oportunidades y amenazas.
- Cumplimiento de las exigencias legales y reglamentarias, así como de las normas internacionales.
- Mejora de la información financiera.
- Mejora de la gobernabilidad.
- Mojera de la confianza de los grupos de interés (*stakeholder*)
- Establecimiento de una base confiable para la toma y planificación de las decisiones.
- Mejora de los controles.
- Asignación y uso eficaz de los recursos para el tratamiento del riesgo.
- Mejora de la eficacia y eficiencia operacional.

- Mejora de la salud, de la seguridad y de la protección del medio ambiente.
- Mejora de la prevención de pérdidas y de la gestión de incidentes.
- Minimiza las pérdidas.
- Mejora del aprendizaje organizacional
- Mejora de la capacidad de recuperación de la empresa.

IV. Ley n.º 29733: Protección de datos personales

Es importante precisar los derechos de los datos personales del propietario informándole sobre el enfoque que se les dará a sus datos, así como el acceso a las bases respectivas para actualizar, incluir, rectificar, suprimir datos e impedir su suministro a terceros que puedan afectar los derechos constitucionales. Los datos personales tienen un anuncio enumerativo de las clases de información que son consideradas como personales: nombre, teléfono, dirección, fotografía, huellas dactilares, entre otros. De igual manera, este tipo de datos permite la interacción con otras personas, o con una o más organizaciones. Por otro lado, los datos sensibles son aquellas características físicas y emocionales o aquellas circunstancias de la vida familiar o afectiva; en este caso, la Ley exige que el consentimiento de los datos sensibles sea por escrito mediante una firma manuscrita, una firma digital o cualquier otro mecanismo de autenticación.

La Ley de la Autoridad Nacional de Protección de Datos Personales, dependiente del Ministerio de Justicia de Perú[14] implica que toda empresa o persona que trabaje con información deberá facilitar su base de datos (incluyendo el consentimiento de los titulares) al regulador.

V. Estructura

Está estructurado en un título preliminar con disposiciones generales, seis títulos, 131 artículos, tres disposiciones complementarias

14 El Peruano. *Ley n.º 29733 Ley Protección de Datos Personales*, Lima, Congreso de la República del Perú, 2011, disponible en [https://leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf].

finales, dos disposiciones complementarias transitorias, que dispone lo siguiente:

1. El tratamiento de datos personales deberá realizarse con pleno respeto de los derechos fundamentales de sus titulares, garantizándose en su mayoría el derecho fundamental a la protección de los datos personales previsto en la Constitución Política de Perú, en un marco de los demás derechos fundamentales que en ella se reconocen.
2. Limitaciones al ejercicio del derecho fundamental a la protección de datos personales solo pueden ser establecidas por ley, al respetar su contenido esencial y estar justificadas en razón del respeto de otros derechos fundamentales o bienes según la Constitución protegidos.
3. Las comunicaciones, telecomunicaciones, sistemas informáticos o sus instrumentos, cuando sean de carácter privado o uso privado, solo podrán ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez o con autorización de su titular, con las garantías previstas en la ley. Se guardará secreto de los asuntos ajenos al hecho que motiva su examen. Los datos personales obtenidos con violación de este precepto carecerán de efecto legal.
4. Se debe guardar secreto de los asuntos ajenos al hecho que motiva su examen y los datos personales obtenidos con violación de este precepto carecen de efecto legal.
5. La mencionada ley también ha establecido limitaciones al consentimiento para el tratamiento de datos personales. En ese sentido, no se requerirá el consentimiento del titular de datos personales en los siguientes casos:

- Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.
- Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.
- Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley.

- Cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.
- Cuando se trate de datos personales relativos a la salud y sea necesario en circunstancia de riesgo para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.
- Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos.
- Cuando se hubiera aplicado un procedimiento de anonimización o disociación.
- Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de datos personales.
- Otros establecidos por ley, o por el reglamento otorgado de conformidad con la presente Ley[15].

15 El Peruano. *Ley n.º 29733 Ley Protección de Datos Personales*, (2011), Lima, Congreso de la República del Perú, disponible en [https://diariooficial.elperuano.pe/pdf/0036/ley-proteccion-datos-personales.pdf].

VI. Controles de seguridad

Los controles de seguridad son aquellas medidas preventivas y reactivas de los sistemas tecnológicos de las empresas que permiten el resguardo y la protección de la información teniendo como base los conceptos de confidencialidad, integridad y disponibilidad que son comunes en el ámbito de la seguridad. Del mismo modo, son aquellos mecanismos que son usados para el control y protección de los accesos a los recursos indicados. Los controles deben estar construidos en base a áreas o procesos y objetivos de control de los cuales se deben desprender las actividades y al final los controles en sí[16].

Por otra parte, se le aplican al activo los controles para establecer los parámetros establecidos y los encargados de la seguridad informática empresarial con los responsables del diseño, la configuración y el cumplimiento de los diferentes tipos de controles que varían de acuerdo a diversos factores como la naturaleza del negocio, el tipo de usuario, el presupuesto, la criticidad del activo, etc. Por otro lado, la administración de las empresas son las que deciden cómo será el rol de la seguridad dentro de la empresa.

A. Tipos de controles

– Controles físicos

Son las aplicaciones de medidas de seguridad en una estructura definida usada para prevenir o detener el acceso no autorizado a material confidencial. Algunos ejemplos son: cámaras de circuito cerrado, sistemas de alarmas térmicas o de movimiento, guardias de seguridad, puertas de acero con seguros especiales y biométrica.

– Controles lógicos

Se basan en la tecnología para el control de acceso y el uso de datos confidenciales a través de una estructura física y sobre la red. Incluyen: en-

16 A. Consulting. *Controles Generales TI*, 2013.

criptación, tarjetas inteligentes, autenticación a nivel de la red, Listas de control de acceso –ACLs–, *software* de auditoría de integridad de archivos.

– Controles administrativos

Definen los factores humanos de la seguridad. Aquí se incluye al personal de la empresa y se determinan aquellos usuarios que tienen acceso a algún recurso e información al usar cualquiera de estos medios: entrenamiento y conocimiento; planes de recuperación y preparación para desastres; estrategias de selección de personal y separación; registro y contabilidad de personal.

B. Tecnologías de Información y Comunicación –TIC–

Las TIC permiten la transmisión, el procesamiento y la difusión de la información de manera instantánea, consideradas como base para la reducción de la Brecha Digital sobre la que se tiene que construir una Sociedad de la Información y una Economía del Conocimiento. De esta manera, con el propósito de enfrentar de manera correcta los casos de desastre, se deben diseñar controles para que abarquen a todos los procesos que se manejan en una empresa a través de las TICs, de manera adecuada y con la relevancia que requiere la empresa.

1. Infraestructura y arquitectura tecnológica

Están compuestas por las instalaciones físicas, los servicios y el manejo de los recursos tecnológicos. Sus componentes principales son: *hardware*, *software*, redes e instalaciones de comunicación (internet e intranet), base de datos y personal de administración de información.

2. Tipos de arquitectura

La arquitectura está dedicada a comprender los componentes de los Sistemas de Información en base a una infraestructura organizacional. Existen tres tipos:

– Arquitectura centralizada

Se centran alrededor de una computadora principal que proporciona la potencia computacional y el almacenamiento interno. Constituido por máquinas que alimentan, distribuyen, almacenan o comunican información[17].

– Arquitectura no Centralizada

Son descentralizadas o distributivas.

Cómputo Descentralizado: divide el cómputo centralizado en partes de forma funcional equivalentes en donde cada parte es en esencia un subsistema centralizado más pequeño.

Cómputo Distributivo: divide el cómputo centralizado en muchas computadoras que tal vez no sean de forma funcional equivalentes.

– Arquitectura cliente/servidor

La conexión creciente entre las computadoras condujo a un nuevo tipo de relación, los servidores satisfacen las necesidades de datos y de procesamiento de los clientes (centralizada). Un cliente puede llevar cómputo controlado a nivel local en forma directa al escritorio del usuario, mientras sigue compartiendo los recursos de cómputo, dispositivos, datos con otros usuarios. La independencia proporcionada a los sistemas cliente/servidor, brindan la capacidad para reconfigurar sin demora todo tipo de información[18].

3. Indicadores

1. Clave básico: proporción de empresas que utilizan computadoras e Internet, proporción de empresas con presencia en la web e Intranet.

17 Ibíd.
18 Ibíd.

2. Clave extendido: proporción de empresas que utilizan Internet clasificado por tipo de acceso y por tipo de actividad, proporción de empresas con red de área local –LAN– y extranet.

4. Impacto

En la actualidad, se requiere no sólo un simple dominio técnico de la tecnología sino de una reflexión sobre el potencial y el impacto que produce el conocimiento de las tecnologías en los sistemas informáticos que se producen y las relaciones que existen entre los componentes de *hardware* y *software*. Si se llegase a tener poco dominio, se pueden estructurar unos componentes de *hardware* o de *software* poco robustos, que conllevarían al decaimiento repentino de una gran cantidad de sistemas o a que una empresa tenga sistemas de difícil mantenimiento.

C. Algoritmos y criptografía

Analiza aquellos procedimientos y métodos para modificar los datos con la finalidad de alcanzar algunas propiedades de seguridad, tales como:

- *Confidencialidad*: Garantía de que las personas autorizadas tengan acceso a la información.
- *Integridad:* Garantía de que el documento original, tanto público como confidencial, no ha sido modificado.
- *Autenticación*: Garantía de la identidad del titular de la información.

El objetivo de un algoritmo criptográfico es desencriptar los datos sin necesidad de usar la llave. Si se hace uso de un buen algoritmo de encriptación, no hay ninguna técnica significativa mejor que intentar de forma metódica con cada llave posible[19].

19 Ibíd.

D. Clasificación de los algoritmos criptográficos de seguridad

a) Criptografía de clave secreta o simétrica: Aquí se incluye el conjunto de algoritmos diseñados para cifrar un mensaje haciendo uso de una única clave conocida por los dos interlocutores, de manera que el documento cifrado sólo pueda descifrarse conociendo dicha clave secreta. Algunas de sus características son:

- No se puede obtener el mensaje original ni la clave que se ha utilizado por medio del mensaje cifrado, aunque se conozcan todos los detalles del algoritmo criptográfico utilizado.
- Se utiliza la misma clave tanto para cifrar el mensaje original como para descifrar el mensaje codificado.
- Emisor y receptor deben acordar una clave común a través de un canal de comunicación confidencial antes de poder intercambiar información confidencial por un canal de comunicación inseguro.

Los algoritmos simétricos más conocidos son:

DES: Es un sistema de cifrado simétrico por bloques de 64 bits, en donde ocho bits son utilizados como un control de paridad para la verificación de la integridad de la clave. Se encarga de combinar, sustituir y permutar entre el texto a cifrar y la clave de forma que asegura que las operaciones puedan realizarse en ambas direcciones (para el descifrado).

3 DES: aunque una clave de 56 bits ofrece una enorme cantidad de posibilidades, muchos procesadores pueden calcular más de 106 claves por segundo. Por lo que, cuando se utilizan al mismo tiempo una gran cantidad de máquinas, es posible que un gran organismo encuentre la clave correcta. Una solución a corto plazo requiere que se encadenen tres cifrados *DES* mediante dos claves de 56 *bits* (esto equivale a una clave de 112 bits).

RC2: Reemplazó a la encriptación *DES* a finales de los 80. Este algoritmo encripta datos en bloques de 64 bits y la clave tiene un tamaño variable de 8 a 128 bits. Lotus Development le pidió ayuda a Rivest en crear el algoritmo RC2 para el software de la compañía Lotus Notes.

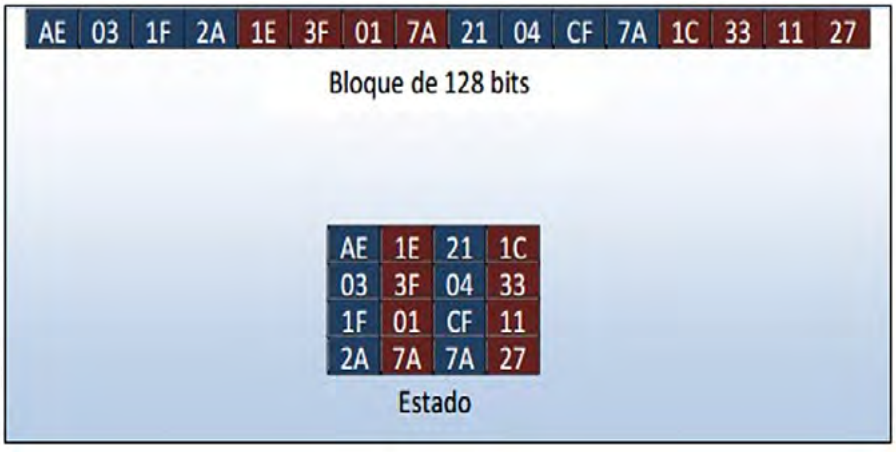
RC4: Es el sistema de cifrado de Flujo Rivest Cipher más utilizado y se emplea en algunos de los protocolos más populares como Transport Layer Security –TLS/SSL– para proteger el tráfico de Internet y Wired Equivalent Privacy –WEP– para añadir seguridad en las redes inalámbricas.

RC5: Tiene tamaño variable de bloques (32, 64 o 128 bits), con tamaño de clave (entre 0 y 2040 bits) y número de vueltas (entre 0 y 255). La combinación sugerida en primer lugar era: bloques de 64 bits, claves de 128 bits y 12 vueltas. Una de sus características más es el uso de rotaciones dependientes de los datos; también contiene algunas unidades de sumas modulares y de Puertas O-exclusivo –XOR–.

Blowfish: Divide los mensajes en bloques de tamaños iguales de hasta 64 bits y los encripta. El tamaño de la clave es de 32 a 448 bits. SCHNEIER lanzó Blowfish como un algoritmo de dominio público y de libre acceso para cualquier persona que desee encriptar datos.

AES: Algoritmo de cifrado por bloques que fue en principio diseñado para tener longitud de bloque variable, pero el estándar define un tamaño de bloque de 128 *bits*, por lo tanto, los datos a ser encriptados se dividen en segmentos de 16 bytes (128 bits) y cada segmento se puede ver como una matriz de 4x4 bytes al que se llama estado. En la Figura 10 se ve su organización.

Figura 10
Organización del Cifrado AES



Fuente: CISCO, 2010.

b) Criptografía de clave pública o asimétrica: Incluye un conjunto de algoritmos criptográficos que utilizan dos claves distintas para cifrar y para descifrar el mensaje. Ambas claves tienen una relación matemática entre sí, pero su seguridad parte del conocimiento de que una de las claves no permite descubrir cuál es la otra clave. Algunas de sus características son:

- Se utilizan una pareja de claves denominadas clave pública y clave privada, pero a partir de la clave pública no es posible descubrir la clave privada.
- A partir del mensaje cifrado no se puede obtener el mensaje original, aunque se conozcan todos los detalles del algoritmo criptográfico utilizado y aunque se conozca la clave pública utilizada para cifrarlo.
- Emisor y receptor no requieren establecer ningún acuerdo sobre la clave a utilizar. El emisor se limita a obtener una copia de la clave pública del receptor, lo cual se puede realizar, en principio, por cualquier medio de comunicación, aunque sea inseguro[20].

E. Criptografía

Su objetivo principal es garantizar la confidencialidad de los documentos, aunque sean accesibles a personas que no estén autorizadas, se utiliza más que todo en la transferencia de información por canales de comunicación no seguros como el Internet. Además, estas técnicas garantizan la integridad ya que el documento no puede ser modificado. Los algoritmos de cifrado forman un papel importante en la transferencia de archivos y de información durante el acceso a una página web de un banco, y también protegen archivos importantes, en caso de acceso ilegal, dentro del disco duro o el cualquier medio de almacenamiento digital.

20 Ibíd.

F. Base de Datos

Los datos sensibles están, en su mayoría, almacenados en sistemas gestores de bases de datos como Oracle o Microsoft, por lo que el ataque a cualquiera de las bases de datos es uno de los objetivos de los cibercriminales produciendo una debilidad en los navegadores web y en los gestores de base de datos. Para evitar estas complicaciones, se debe considerar que la administración de la seguridad de los datos en una empresa es una tarea compleja y que la apertura de las bases de datos corporativas a Internet incrementa los riesgos de ataque.

G. Conectividad

Debido a la explosión de servicios de datos ofrecidos por estas redes, se ha incrementado la dependencia de los usuarios y de las empresas de la trasmisión de datos al despertar una conciencia en cuanto a la necesidad de proteger la información y de garantizar la autenticidad de dicha información. La seguridad de las redes determina el funcionamiento óptimo de todas las máquinas de una red y que todos sus usuarios tengan los derechos que se les han concedido. Esto incluye evitar que las personas no autorizadas intervengan con malicia en el sistema, evitar que los usuarios hagan operaciones que puedan dañar el sistema, fortalecer los datos a través de la previsión de fallas y verificar que no haya interrupciones de los servicios.

VII. Recuperación de Datos

A. Beneficios de un Plan de Recuperación por Desastre

- Evita o mitiga el impacto de ciertos riesgos, al minimizar las potenciales pérdidas económicas y mejora la capacidad de recuperar las operaciones normales del negocio.
- Minimiza la probabilidad de interrupción de las funciones críticas y recupera las operaciones lo que asegura la estabilidad organizacional.

- Identifica los sistemas críticos y sensitivos que constituye una empresa.
- Proporciona un procedimiento planificado al minimizar el tiempo de toma de decisiones en caso de ocurrir un desastre.
- Elimina la confusión de los usuarios y reduce la probabilidad de equivocación debido al estrés que produce una crisis.
- Protege los activos de la empresa.
- Minimiza potenciales responsabilidades legales.
- Proporciona materiales de entrenamiento para el personal.

B. Procesos principales en la creación de un Plan de Recuperación

1. Análisis de riesgos –AR– y análisis de impacto al negocio –BIA–

El proceso de análisis de riesgos provee la base del plan de recuperación e identifica las posibles amenazas que podría traer un impacto dentro de la empresa. El razonamiento con respecto a las posibilidades de crisis le permite a la compañía una visión de lo que puede ser importante al dar como resultado mejores planes de contingencia.

Como complemento, el análisis de impacto de negocio –BIA– determina el efecto que tiene cada tipo de amenaza potencial sobre las funciones o las áreas de la empresa como puede ser servicio al cliente, operaciones internas, asuntos legales y asuntos financieros. Este análisis es la clave para desarrollar la mayoría de los objetivos de un plan de recuperación por desastre.

Un análisis de riesgos –AR– y un análisis BIA tienen cuatro objetivos fundamentales que son:

1. Identificación de los activos de la compañía y de las funciones necesarias para la recuperación de datos en caso de desastre, priorizándola de acuerdo a su criticidad –BIA–.
2. Identificación de las amenazas probables a los activos y a las funciones –AR–.
3. Elaborar objetivos para la creación de estrategias que eliminen los riesgos y minimicen el impacto de aquellos riesgos que no se pueden eliminar –AR–.

4. Elaborar objetivos para la creación de estrategias para el respaldo y/o recuperación de aquellas funciones que son críticas para el negocio y que podrían verse afectadas en un desastre.

2. Identificación y priorización de las funciones operacionales

Basado en el procesamiento de datos, las aplicaciones se clasifican según el siguiente espectro de tolerancia:

Críticas: No se ejecutan a menos que se tenga un ambiente idéntico al de la operación normal de la compañía y no pueden ser reemplazadas por métodos manuales bajo ninguna circunstancia; su tolerancia a la interrupción es muy baja y el costo muy alto. Bajo estas características, la estrategia para recuperar estas aplicaciones debe tener en cuenta el equipo necesario en un sitio alterno y un sistema de respaldos que se pueda cargar en este equipo de manera que se pueda reiniciar la funcionalidad afectada.

Vitales: No se ejecutan por medios manuales o al menos sólo pueden ejecutarse de manera manual por un periodo corto de tiempo. Tienen un poco más de tolerancia a la interrupción y se recuperan en menos de cinco días sin tener mayores contratiempos.

Sensitiva: Se ejecutan por medios manuales con dificultad, pero a un costo tolerable durante un periodo de tiempo más largo.

No Críticas: Pueden ser interrumpidas por un periodo de tiempo extenso a un bajo costo para la compañía.

3. Identificación de las amenazas a los activos y a las funciones

Una vez identificada la criticidad de las funciones, el siguiente paso es realizar un análisis de riesgo e identificar las amenazas existentes en las actividades del negocio. El mejor método de identificación de amenazas es buscar el fenómeno, aparte del origen, que provocaría la pérdida de la funcionalidad normal del sistema. Otras consideraciones para determinar la probabilidad de un desastre específico pueden ser: localización geográfica; topografía del área; proximidad a fuentes de poder, fuentes

de agua o aeropuertos; grado de accesibilidad a la organización; historial de interrupciones y del área a las amenazas naturales.

4. Identificación de los medios de almacenamiento de datos y los sitios de recuperación

Uno de los pilares fundamentales para un plan de recuperación es tener un respaldo actualizado de programas críticos y de datos que pueden ser utilizados en caso de desastre. Existen diversas estrategias para respaldar los activos de una empresa como pueden ser:

a) Respaldo de datos: Es una copia de un conjunto de información específico. Los respaldos por lo común son guardados en cintas o discos que se almacenan en un sitio diferente al sitio donde se ubican los datos operativos de manera que puedan sobrevivir a un desastre que haya destruido la fuente de datos principales. En general, la estrategia de respaldos debe formularse para cumplir con los siguientes objetivos:

- Entender los objetivos de negocio de forma que se cuente con un ambiente de respaldo y recuperación de datos acorde a estos objetivos.
- Permitir que los servicios de información puedan ser reiniciados tan rápido como de manera física sea posible, luego de alguna falla en los sistemas de información.
- Permitir un acceso a los datos respaldados acorde a las necesidades del negocio.
- Cumplir con las políticas regulatorias y de negocio en cuanto a los requerimientos de retención de datos.
- Cumplir con las metas de recuperación de datos en caso de desastre permitiéndole al negocio volver a su estado normal.

Por otro lado, se deben tomar en cuenta estos factores a la hora de diseñar o actualizar una estrategia de respaldos y recuperación de información:

- Capacidad para respaldar todos los datos.

- La frecuencia de respaldo es en esencia un balance entre recursos (redes, procesador, equipo, acceso a las aplicaciones) y la necesidad de datos actualizados.
- Integración de todos los sistemas administradores de datos.
- Disponibilidad continua.
- Administración de los medios.

b) Almacenamiento en sitio alterno: Esto es un asunto clave en el éxito de un plan de recuperación por desastre. Se debe respaldar la información y los activos de una empresa en un sitio seguro y diferente al principal para garantizar que éstos no sean destruidos durante el desastre.

5. Creación del plan de validación o simulación del DRP

Un plan de recuperación por desastre es un documento vivo que debe actualizarse cada vez que se amerite de manera que refleje aquellos cambios en las actividades de la empresa y cambios de personal. Las mejores prácticas establecen que un plan se debería actualizar al menos una vez al año, sin embargo, puede que las condiciones de la empresa requieran que se hagan revisiones más constantes. De esta manera, se determina que un plan debe ser actualizado cuando:

- Hay cambios en el núcleo del sistema, tecnología o procesos de negocio.
- Hay un incremento de la dependencia en la existente o nueva tecnología.
- Hay una reestructuración organizacional.
- Hay un interés, por parte del cliente, reguladores o inversionistas, en los esfuerzos relacionados con el DRP.
- Hay una pérdida económica.
- Hay caídas del sistema.
- Hay un incremento en las amenazas de desastre.
- No hay una actualización en el último año del plan.

Las pruebas permiten un alto grado de confiabilidad en la eficiencia del plan. Cada problema es diferente, pero un plan que ha sido actuali-

zado con constancia tiene más probabilidades de ser exitoso cuando la situación lo requiera. Los beneficios más importantes que se obtienen al probar el plan son:

- Eficiencia y eficacia del plan.
- Identificación de planes de contingencias desconocidos.
- Verificación de la disponibilidad de recursos.
- Se garantiza la verdadera duración del tiempo de recuperación.
- Se entrena al personal asignado a roles de recuperación.
- Permite que el personal se identifique mejor con el plan de recuperación.
- Se establecen las mejoras y las debilidades necesarias del plan.

Los pasos para construir un plan de recuperación son:

Definir los objetivos de las pruebas: al probar que el plan funciona, se verifica que el sitio alterno cumpla con las necesidades del DRP, identifica las deficiencias y omisiones del DRP, proporciona entrenamiento, define el personal requerido y el cronograma de las pruebas, y determina la metodología de las pruebas por medio de una:

a) Revisión Estructural: Se forma un equipo de pruebas que analizará en detalle la totalidad del plan lo que asegura que cada paso esté bien escrito y se entienda.
b) Checklist: Se distribuyen copias del plan a cada equipo lo que permite su revisión y verifica que el plan contenga todas las actividades necesarias.
c) Pruebas de simulación: Es una simulación que consiste en instalar los equipos y sistemas en el sitio alterno, donde las áreas operativas y de soporte se juntan para ejecutar el plan.
d) Pruebas paralelas: Consiste en instalar el equipo y los sistemas críticos en el sitio alterno y verificar que el plan funciona en efecto.
e) Pruebas de interrupción completa: En esta prueba, las operaciones normales son suspendidas por completo y la operación se traslada al sitio alterno al usar el material y personal disponible en el sitio remoto según el plan.

Definición de los resultados esperados de las pruebas: Para determinar la efectividad del DRP los resultados de las pruebas deben ser medidos contra resultados esperados que fueron predefinidos. Si los resultados no son los esperados se puede bajar la expectativa de los resultados o incrementar la efectividad de los procedimientos de prueba.

*Planeación anticipada de los ejercicios de prueba***:** Se debe escribir el plan de pruebas del DRP, también se deben detallar los pasos exactos que se seguirán durante la fase de pruebas, el personal o departamento involucrado y los resultados esperados.

1. Coordinación, ejecución y documentación del plan de pruebas
2. Evaluación de los resultados

6. Roles y responsabilidades

Cada riesgo necesita un personal a cargo y cada acción debe tener un supervisor para asegurarse de que el riesgo está siendo atacado en la forma apropiada. Cada uno de esos roles debe tener las responsabilidades publicadas. Los roles pueden ser de tiempo completo o en parte, de acuerdo al tamaño, complejidad y criticidad del proyecto[21].

21 TechTarget. *Tecnologías actuales de respaldo y recuperación de datos con protección continua de datos (CDP)*, 2009, disponible en [https://searchdatacenter.techtarget.com/es/noticias/2240170035/Tecnologias-actuales-de-respaldo-y-recuperacion-de-datos-con-proteccion-continua-de-datos-CDP].

Capítulo tercero
Una visión global sobre las características de los protocolos de internet y los casos de desastre

Las direcciones IP son aquellas que identifican cada uno de los dispositivos electrónicos en una red. La asignación, el reciclaje y la documentación de direcciones y de subredes en una red, pueden llegar a ser muy confusas de inmediato si no se ha trazado un plan de direccionamiento. Un buen plan ayuda a preparar la base de red para soportar servicios adicionales como unificar las comunicaciones, el acceso inalámbrico y la mayor seguridad de la red. CISCO[22], argumenta que el direccionamiento IP proporciona la base para todos los demás servicios de red y de los usuarios debido a que, sin la base, no sería posible interactuar con la red y los servicios de telefonía IP, correo electrónico, etc. Es con el nacimiento del Internet, que nacen las direcciones IP; primero se origina el protocolo IPv4 y, a medida que se hacen actualizaciones al internet, se origina el IPv5, al dar paso a lo que se utiliza ahora mismo que es el IPv6, protocolo de internet que tiene más capacidad de espacio de direcciones y tamaño permitiéndole a los profesionales poder tener las disposiciones para navegar en las redes sin mucha dificultad. Siguiendo las normas de gestión de las direcciones IPv4 e IPv6, se evita la superposición, los problemas en la sumarización, el desperdicio de las direcciones IP y la complejidad innecesaria.

---

22 CISCO. *Testing IPV4*, 2017, disponible en [https://www.cisco.com/c/en/us/products/ios-nx-os-software/ip-services/index.html?dtid=osscdc000283].

I. Protocolo de Internet Versión 4 (IPv4)

Las direcciones IPv4 son aquellas que contienen 32 bits de longitud, que a su vez están divididos en cuatro octetos de ocho bits; cada octeto tiene un decimal valor de 0 a 255 o un valor binario de 00000000 a 11111111. Por regla general, estas direcciones se muestran en notación decimal, como, por ejemplo, la dirección IP en notación binaria 11 000000.10101000.0000101.00000001, se convierte en 192.168.5.1. cisco[23] señala que todas las direcciones IP contienen un prefijo de red y una porción *host*; aquellos bits de dirección que componen el prefijo de red están determinados por una máscara de subred, y aquellos bits que restan se utilizan para los hosts. En la Tabla 5 se muestra la dirección IP expresado en binario y en decimal:

Tabla 5
Dirección IP en Binario y Decimal

Type	Binary notation	Dotted decimal notation
IP address	11000000.10101000.00000101.00000001	192.168.5.1
Subnet mask	11111111.11111111.11111111.00000000	255.255.255.0
Network	11000000.10101000.00000101.00000000	192.168.5.0
Host	00000000.00000000.00000000.00000001	0.0.0.1

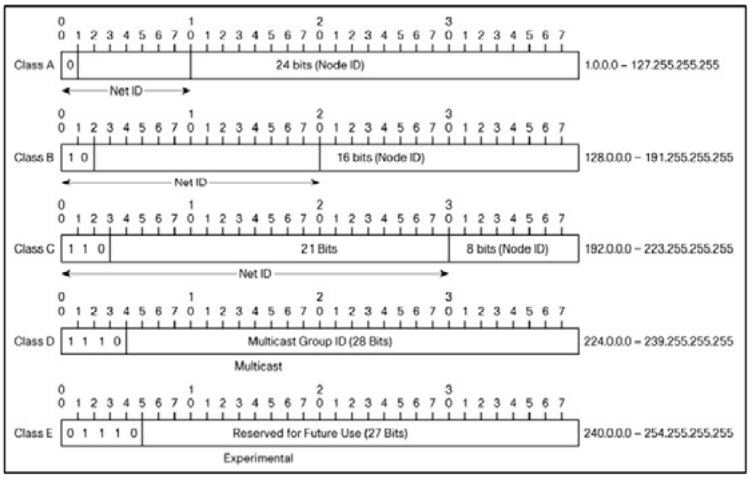
Fuente: cisco, 2008.

A. Clases de direccionamiento

Al comienzo, las direcciones se dividieron en varias categorías diferentes o en clases basadas en la cantidad de bits de la dirección que se utiliza para el prefijo de red y cuántos bits se utiliza para los hosts. El direccionamiento basado en clases está definido como A, B, C, D y E. Las clases A, B y C son empleadas para la creación de redes en general, la clase D fue designada para el tráfico IP Multicast y la clase E se separó para el uso experimental.

23 Ibíd.

Figura 11
Clases de Red



Fuente: CISCO, 2008.

Como se observa en la Figura 11 los prefijos para las direcciones en las clases A, B y C se caracterizan por lo siguiente:

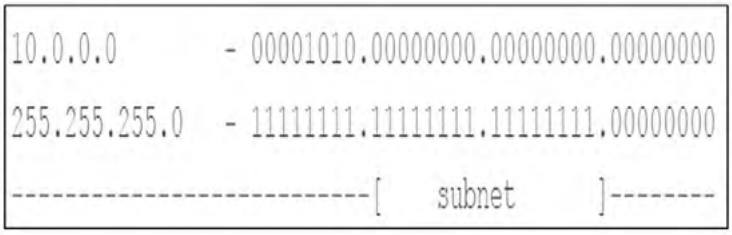
- En las direcciones de clase A, el primer octeto es el prefijo de red y los tres octetos restantes son *hosts*.
- En las direcciones de clase B, los primeros dos octetos son el prefijo de red y los restantes dos octetos son *hosts*.
- En las direcciones de clase C, los primeros tres octetos son el prefijo de red y el octeto restante es el *host*.

B. Subneteo y Superneteo

El Subneteo es el que permite crear múltiples redes lógicas que existen dentro de una clase A, B, C o red única; es imperativo afirmar que no sería muy útil crear una sola red de clase A, B o C sin subredes. Por consiguiente, el Subneteo es el que permite a las redes principales (clase A, B o C) dividirse en subredes más pequeñas. Por ejemplo, en lugar de tener una sola red con 16 millones de hosts, una clase A podría dividirse en 65.535 redes, cada una con 254 direcciones de host; este es un tamaño más práctico de la red para la mayoría de las organizaciones. En la

subred de una red se utilizan aquellos bits de la porción de host de una dirección para crear subredes adicionales, esto quiere decir que, si en la clase A se toman 16 bits de la porción de hosts de una dirección en concreto, y el segundo y el tercer octeto se utilizan para crear subredes, se pueden hacer un gran número de redes más pequeñas permitiendo un diseño de la red más flexible y más práctico. Sin embargo, la clase A 10.0.0.0 tiene una máscara de 255.0.0.0 que, con frecuencia, se le llama su máscara natural; y cuando se utilizan los próximos 16 bits como la subred se da una máscara de 255.255.255.0 o /24, lo que ahorraría los últimos 8 bits para direcciones de hosts, al dar 10.0.0.0-10.0.0.255 para las direcciones de la red 10.0.0.0/24.

Figura 12
Subneteo



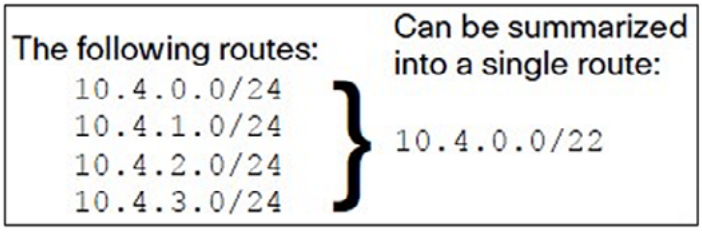
Fuente: CISCO, 2008.

En la Figura 12 se muestra en el lado izquierdo de la red 255.255.255.0 10.0.0.0 y la máscara de subred se muestra en notación decimal, y en la derecha se muestran sus homólogos binarios.

Por otra parte, la sumarización de red (Superneteo) permite la creación de una ruta única que resume compuesto por un bloque de contiguas subredes. En una red sin resumen, existe una ruta para cada subred en el proceso de enrutamiento en cada *router* en la red al causar que, en primer lugar, las redes con un gran número de subredes tengan un gran número de rutas que puede utilizar una gran cantidad de memoria y de CPU y, por ende, degradar el rendimiento de los *routers*; en segundo lugar, que cada vez que una subred se agregue o se elimine de una red, los *routers* tengan que volver a calcular la tabla de enrutamiento. A menudo, las rutas no se agregan o se quitan en una red estable. Sin embargo, esto no resultar ser un problema, sino una WAN poco

fiable o router defectuoso que puede causar una ruta "flap" al causar reconvergencia frecuente de la tabla de enrutamiento e inestabilidad de la red. En la Figura 13 se muestra la sumarización de rutas.

Figura 13
Sumarización de Rutas



Fuente: CISCO, 2008.

C. Modos de comunicación

El protocolo de Internet Versión 4 (IPv4) maneja tres modos principales de comunicación: *Unicast*, *Broadcast* y *Multicast*.

– *Unicast*

Aquí se observa la transmisión única e independiente de información de un equipo a otro; si un equipo desea transmitir la misma información a otro equipo diferente tendría que mandar una copia por separado al segundo equipo y así cada vez más. Se puede hacer un ejemplo con la comunicación humana en donde un grupo va a hacer una fiesta y para que vaya la gente necesita transmitir los detalles de la reunión, en un modo de comunicación *Unicast*, el grupo iría a cada uno de sus conocidos y le contaría los detalles a cada uno por separado. Esto supone un trabajo agotador y muy pesado de realizar, pero se logra transmitir el mensaje final.

– *Broadcast*

Este modo de comunicación se define como la dirección que todos los equipos deben procesar aparte de la dirección IP que está configurada

en la tarjeta de red; cuando se manda tráfico a la dirección *Broadcast* de una red, todos los equipos la reciben, la analizan y, en caso necesario, trabajan con ella. Refiriéndose al ejemplo anterior de la fiesta, en lugar de hablar con cada uno de los conocidos, el grupo va a una oficina, toma un micrófono y grita los detalles de la fiesta a todos los presentes; el mensaje solo es transmitido una vez, pero todos los presentes reciben y procesan la información. Por supuesto, habrá personas a las que no les interesa saber de la fiesta, pero igual se enteraron.

– *Multicast*

En este método de comunicación, el equipo transmite una sola copia del mensaje a unos equipos selectos y específicos. En esta ocasión se hará el ejemplo de un grupo que tenga un programa de radio o de televisión donde sus conocidos sintonizan sin parar; es en este programa donde el grupo da los detalles de la fiesta, pero sólo las personas que están interesadas son las que reciben el mensaje final.

II. Protocolo de Internet Versión 6 (IPv6)

Las direcciones IP versión 6 son aquellos identificadores de 128 *bits* que se utilizan para las interfaces y conjunto de interfaces. Su desarrollo ha estado en marcha desde inicio de la década de los noventa con el lanzamiento de las Request For Comments –RFC– a través de Internet Engineering Task Force –IETF–. Su principal objetivo impulsor para su desarrollo fue el reconocimiento de los espacios limitados de las direcciones IPv4 que se agotan con el tiempo; los modelos actuales muestran que el espacio de las direcciones IPv4 ya ha sido agotado y se reutiliza direcciones asignadas que no se venían usado. CISCO[24] argumenta que hay varios recursos disponibles para ayudar a construir un plan de integración del IPv6 y que el IETF tiene varios RFC que permiten diseñar distintos planes de integración.

---

24 CISCO. *Certificado PKI*, 2011, disponible en [https://www.cisco.com/c/en/us/td/docs/ios/sec_secure_connectivity/configuration/guide/12_2sr/sec_secure_connectivity_12_2sr_book/sec_store_pki_cred.pdf?dtid=osscdc000283].

A. Representación de la dirección

El primer tema que se trata es cómo representar estos 128 bits; es importante considerar que el tamaño del espacio de la numeración, números hexadecimales y los dos puntos (:), fueron elegidos para representar las direcciones IPv6. Un ejemplo de dirección IPv6 es: 2001:0DB8:130F: 0000:0000:7000: 0000:140B. Se tiene en cuenta, entonces, que:

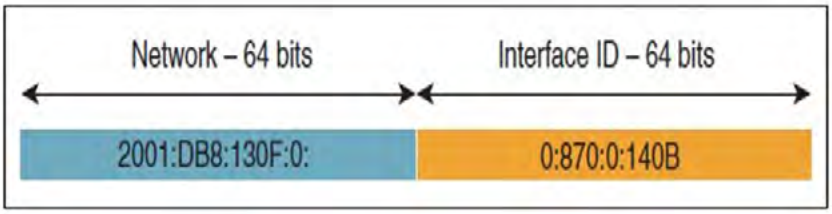
- No hay mayúsculas y minúsculas, es decir, la minúscula "a" significa lo mismo que mayúscula "A".
- Hay 16 bits en cada agrupación entre los dos puntos.
- 8 grupos * 16 *bits* = 128 *bits*.
- Además, existen formas aceptadas para acortar la representación de la dirección, tales como:
- Los ceros iniciales se pueden omitir, por lo que un campo de ceros puede ser representados por un único 0.
- Los ceros finales deben estar representados.
- Campos sucesivos de ceros se puede acortar a ":". Esta representación abreviada sólo puede ocurrir una vez en la dirección.

Al considerar estas reglas, la dirección IPv6 antes indicada puede reducirse a:

1. 2001:0DB8:130F: 0000:0000:7000: 0000:140B
2. 2001: DB8:130F: 0:0:7000: 0:140B (Ceros)
3. 2001: DB8:130F: 0:0:7000: 0:140B (Ceros finales)
4. 2001: DB8:130F: 7000:0:140B (Campos sucesivos de ceros)

Por último, un típico uso de direcciones IPv6 es 64 *bits* para representar a la red y 64 *bits* para representar el identificador de interfaz o *host*. Al utilizar la anterior dirección de ejemplo, los campos de red y un identificador de host se desglosan como se observa en la Figura 14.

Figura 14
Desglose de la dirección



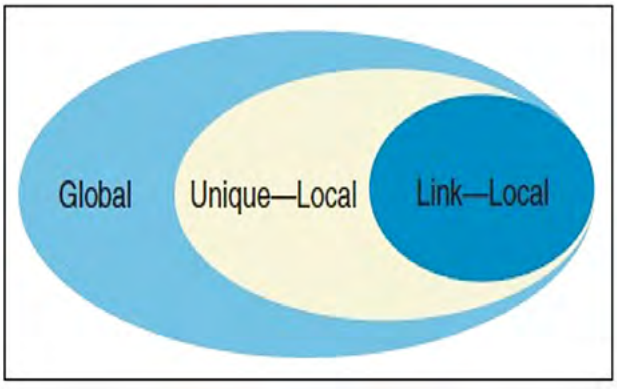
Fuente**:** cisco, 2008.

B. Tipos de direcciones

– Unicast

Una dirección de unidifusión se define como un identificador para una única interfaz. Estas direcciones se utilizan por lo común cuando un sistema final específico necesita comunicarse con otro sistema final específico, es decir, la comunicación en punto a punto. Las direcciones IPv6 *unicast* también tienen un alcance definido como global, *unique* local y *link* local. La Figura 15 muestra el alcance de cada dirección definida.

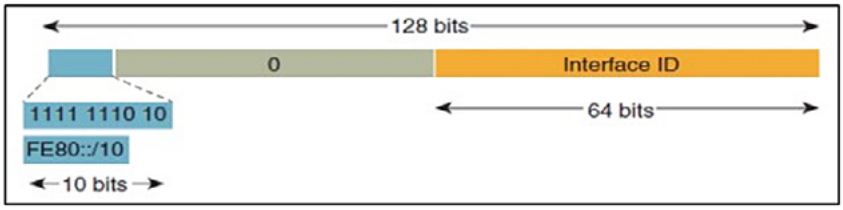
Figura 15
Alcance de cada dirección definida



Fuente: cisco, 2008

Una diferencia clave a destacar es que se espera que una interfaz IPv6 tenga varias direcciones IPv6 asociadas con ella. Este modelo es muy diferente de IPv4, donde una interfaz fue en exclusiva asignada a una única dirección. Las interfaces IPv6 siempre tienen una dirección local de enlace, también tienen un *unique* local o dirección única global y puede tener ambos tipos de direcciones. Por otro lado, un *Link* Local se utiliza para las comunicaciones en un simple enlace y los paquetes con el *link* local fuente o dirección de destino no se reenvían por un *router* de ese enlace; las direcciones link local sólo tienen significado en ese enlace. Todas las direcciones de enlace local se pueden identificar a partir del prefijo FE80: :/10. Como se ha señalado de antemano, todas las interfaces de IPv6 tienen una dirección local de enlace asignado a ellos; en la Figura 16 los últimos 64 bits se designan como ID de interfaz, lo que se define como la parte "host" de la dirección y es una parte de todas las direcciones IPv6 así sean *link* local, *unique* local o *unique* global. De momento, la recomendación de la RFC es utilizar los últimos 64 bits de una dirección IPv5 como el interfaz identificador.

Figura 16
Representación Dirección *Link* Local



Fuente: CISCO, 2008.

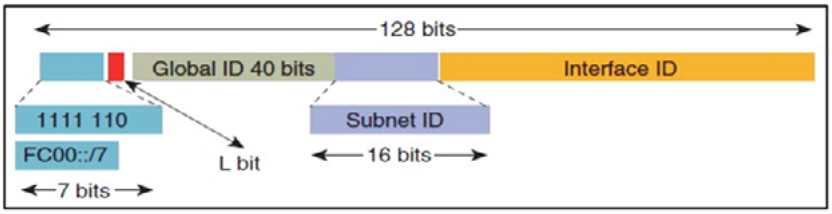
Por otra parte, las direcciones locales únicas son definidas por RFC 4193 (*Unique* Local IPv6 Direcciones *Unicast*) y son accesibles fuera de un enlace en particular, pero sólo tienen sentido dentro de un alcance limitado. Estas direcciones no están ruteadas a través de Internet, sino que deben estar enrutadas dentro de un sitio o un dominio del cliente. Además, son análogas a RFC 1948 direcciones en IPv4 y cuya única diferencia es que el espacio único de direcciones local pretende ser única

a nivel mundial. Estas direcciones son reconocibles porque son todas del bloque de direcciones FC00: :/7.

La Figura 17 muestra el desglose de una dirección local única. El *bit* de L se establece en 1 si la dirección se asigna en el lugar, RFC 4193 reserva el *bit* 0 para uso futuro. Esta definición de bit L quiebra el bloque FC00: :/7 en dos bloques:

1. FC00: :/8 Reservado para uso futuro.
2. FD00: :/8 A nivel local asignado a direcciones unique local.

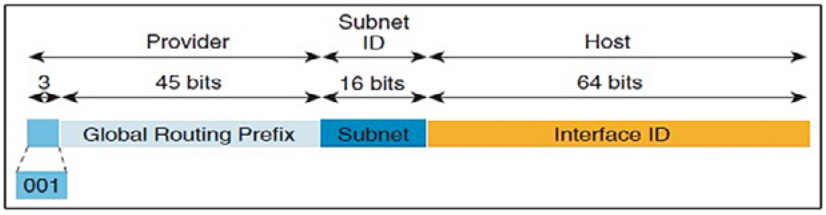
Figura 17
Representación de una Dirección Unique Local



Fuente: CISCO, 2008.

Además, las direcciones globales son accesibles desde todo el Internet, se asignan desde los registros regionales como, por ejemplo, RIPE, ARIN y APNIC. Las direcciones globales están en este momento asignadas del bloque 2000: :/3. En la Figura 18 se observa la representación de una dirección global.

Figura 18
Representación de una Dirección Global



Fuente: CISCO, 2008.

Por consiguiente, en la Tabla 6 se muestran las asignaciones de bloques únicos globales actuales a los registros regionales.

Tabla 6
Unique Global – Asignación de bloques a los registros regionales

BLOQUE DE DIRECCIONES IPV6	REGISTRO REGIONAL
2001:/16	VARIOS
2400:0000: :/12	APNIC
2600:0000: :/12	ARIN
2800:0000: :/12	LACNI
2A00:0000: 1/2	RIPE NCC
2C00:0000: 1/2	AFRINIC

Fuente: CISCO, 2008.

Por último, hay varios bloques de usos especiales o reservados de espacio de direcciones IPv6 que se han definido en múltiples RFC como, por ejemplo, RFC 5156 tiene una lista de las direcciones de uso especial definidos en la actualidad, algunos de los bloques más comunes incluyen:

a) 2001:db8: :/32 Para documentación (RFC 3849)
b) 2002: :/16 Para túnel automático 6to4 (RFC 3964)
c) 2001: :/32 Para mecanismos de túnel Teredo (RFC 4380)

– *Anycast*

Una dirección IPv6 *anycast* es definida como un identificador asignado a múltiples interfaces en diferentes nodos. Aquí las comunicaciones son similares a las comunicaciones *multicast*, pero el modelo es un uno al más cercado de muchos, es decir, que un *host* se comunica a los más cercanos de muchos nodos potenciales. Más cercano es un término relativo y, por lo general, se deja a un protocolo de enrutamiento y sus asociadas métricas para decidir qué dirección *anycast* es más cercana basado en los criterios de selección. Un buen ejemplo para las comunicaciones de difusión ilimitada son los servidores DNS, el *host* que ne-

cesita saber cuál es la dirección para www.xyz.com no le importa qué servidor DNS responde. La máquina que hace la consulta se dirige en lo topológico al servidor más cercano; si el servidor DNS que responde queda fuera de línea, el siguiente servidor más cercano recibe la solicitud. Estas direcciones no pueden distinguirse de las direcciones *unicast* cuando se mira en la misma dirección, es decir, no hay bits definidos que hacen que una dirección se distinga como *anycast*.

– *Multicast*

Las direcciones de multidifusión o multicast se definen como aquellos identificadores para un conjunto de interfaces que pertenecen a menudo a diferentes nodos; se utilizan para identificar los grupos de interfaces que están preparadas para recibir contenidos similares (por ejemplo, video). El modelo de conversación, en este caso, es un modelo de uno a muchos. Además, que estas direcciones están asignadas fuera del bloque FF00: :/8.

Las direcciones de multidifusión también tienen un ámbito asociado con ellos. Los ámbitos son muy similares a los ámbitos definidos por las direcciones únicas:

***Link* Local**: Estas direcciones sólo están destinadas a sistemas en un solo enlace y no deben ser enrutadas por los equipos de red. Este comportamiento es el mismo que las direcciones *unicast link* local.

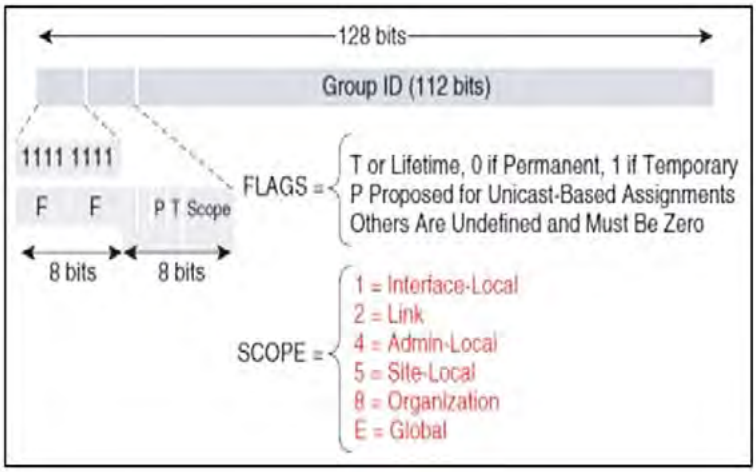
a) Organización: Estas direcciones son para uso dentro de una organización, estas direcciones son similares a las direcciones unicast unique local.
b) Global: Estas direcciones son utilizables a través de Internet similar a la de unidifusión global direcciones únicas.

Así mismo, hay algunos ámbitos definidos para las direcciones IPv6 *multicast*:

1. **Interface Local:** Están destinados a la transmisión de multidifusión dentro de un nodo.
2. **Site Local:** Son para uso en un solo sitio.

Para concluir, hay algunas direcciones de uso multidifusión especiales o reservados similares al espacio de direcciones de unidifusión. En la Figura 19, se mencionan los usos previstos de una pareja de los grupos de multidifusión más comunes.

Figura 19
Dirección IPv6 *Multicast*

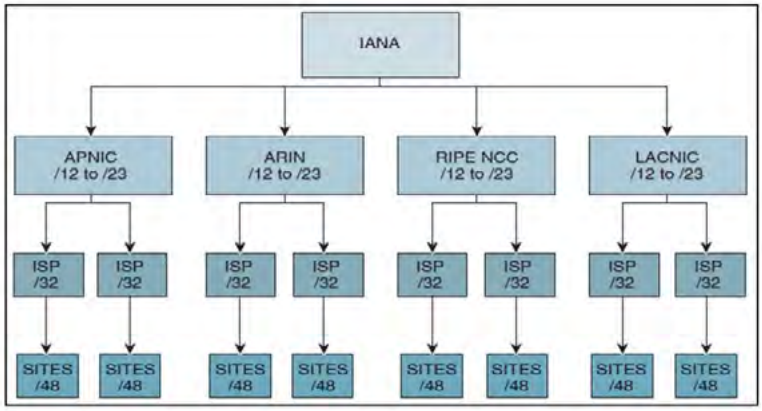


Fuente: CISCO, 2008.

C. Políticas de asignación de direcciones

En la actualidad, IANA asigna bloques de direcciones a los registros regionales, quienes asignan bloques de direcciones a proveedores de servicios; y es responsabilidad del proveedor de servicios distribuir las direcciones a sus clientes respectivos. La política actual varía según la región y, en el caso más conservador, dicta que el usuario final debe ir a través de su proveedor de servicios para lograr obtener el espacio de direcciones IPv6 y no puede acercarse en seguida al registro regional de espacio de direcciones IPv6. En la Figura 20 se muestran los niveles de asignación.

Figura 20
Niveles de asignación de direcciones



Fuente: CISCO, 2008.

D. Planificación de direcciones

– Proveedor de Direccionamiento Independiente

La atracción principal para usar un proveedor de espacio independiente es que una organización no está vinculada por completo a un determinado proveedor, es decir, que puede cambiar de proveedor sin tener que pasar y volver a numerar la totalidad de su red cuando el espacio de direcciones del proveedor cambia. Además, el proveedor de espacio independiente permita a una organización conectarse a múltiples proveedores de servicios con un solo bloque de direcciones IPv6, lo que proporciona resistencia y redundancia en caso de un problema de red de los proveedores de servicios.

– Direccionamiento ULA

Cuando se construye el plan de direcciones IPv6 surge la pregunta sobre si es conveniente o no utilizar una única dirección a nivel mundial. Estas alternativas no son excluyentes entre sí debido a que un punto final IPv6 puede y tiene múltiples direcciones IPv6; de ahí que las direcciones *unique* local y global pueden ser utilizados. Es importante acotar que las direcciones globales se deben utilizar si se desea conectividad a Internet.

– Diseño a nivel de Red

La seguridad es filtrar la Dirección Única Local –ULA– en cualquier límite externo a su organización. A menos que esté permitido en específico por un acuerdo previo, todo el tráfico que tiene una dirección ULA de origen o destino y se origina fuera de la red no se debe permitir en la red.

La solicitud inicial de un bloque de direcciones IPv6 merece atención cuando se construye el plan de direccionamiento, este paso se produce si una organización trata de utilizar un proveedor asignado o un proveedor de espacio independiente.

1. Planificación Inicial de Subredes

Al dar con el tamaño inicial del bloque de direcciones IPv6, se deben tomar en cuenta algunos factores:

a) El tamaño total de la red actual y el crecimiento futuro de una organización debe considerar el tamaño de la red al estimar el tamaño del bloque de direcciones IPv6 que se va a solicitar. El tamaño de la red debería tener en cuenta el número de subredes que es diferente de la planificación de IPv4 basada en el número de sistemas extremos.

b) La estrategia *Multihoming* (múltiples referencias) formula la solicitud inicial de direcciones IPv6, una organización debe tener en cuenta la forma en que se acerca a redundancia y del fracaso de escenarios cuando se conecta a uno o múltiples proveedores de servicios.

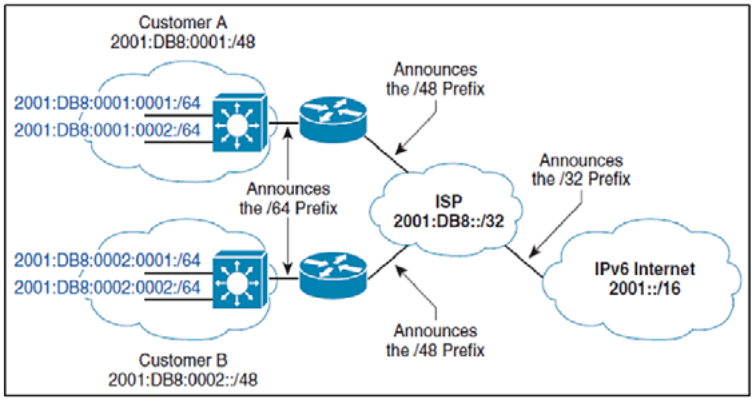
c) Las Organizaciones Multinacionales deben considerar su enfoque cuando solicitan bloques de direcciones de IPv6 debido a la estricta jerarquía que la política de asignación actual impone.

Más aún, una organización debe tomar estas consideraciones si desea solicitar bloques de direcciones IPv6: el tamaño del bloque inicial, manejar la conmutación por error, ingeniería de tráfico y redundancia, y establecer acuerdos con los proveedores de servicios para actualizar sin parar su política referente a los prefijos de longitudes.

2. Agregación de Sub Redes

Una vez definido el bloque de direcciones IPv6 inicial, hay algunos factores a considerar cuando se construye el plan de direcciones. El tamaño actual de la red es una consideración primordial para la construcción del bloque de petición inicial y también es un factor importante cuando se mira en el plan general de subred; el RFC actual sugiere que un prefijo /48 se emita a las organizaciones debido a que el prefijo /48 le otorga 2 ^ 16 (65536) /64 prefijos de usar. Esto demuestra una potencial cantidad para un correspondiente incremento en el tamaño de la tabla de enrutamiento que un dispositivo de red utiliza para enviar paquetes. Otra consideración primaria para la construcción de un plan de direcciones IPv6 es la agregación de prefijos IPv6 que permite a la red escalar y crecer. La Figura 21 muestra una aplicación simple del principio de agregación.

Figura 21
Direccionamiento Jerárquico



Fuente: CISCO, 2008.

3. Desarrollo de Subredes

El crecimiento es otra fase que debe ser considerado en la asignación de subredes en la red. RFC 3531 presenta un plan para la asignación de

subredes basados en límites de *bits* dentro de prefijo IPv6 de la organización y cómo esos límites pueden ser manipulados o cambiados debido a que la red crece y se necesitan más subredes; esto debe contemplarse en el plan de red para acomodar el crecimiento futuro y la adición de más subredes, que puede ser acomodado para salir por los bloques adyacentes de espacio de direcciones reservadas. La Tabla 7 muestra cómo implementar el plan de *networking* con proyección a crecimiento.

Tabla 7
Plan de direccionamiento considerando el crecimiento

Region (4 bits)	Regional Prefix	Facility (4 bits)	Facility Prefix	Subnets per Facility (8 bits)
1 (0000,0001)	2001:db8:1:0::/52	1 (0000)	2001:db8:1:0::/56	2001:db8:1:0::/64 to 2001:db8:1:ff::/64
	2001:db8:1:1::/52	2 (0100)	2001:db8:1:400::/56	2001:db8:1:400::/64 to 2001:db8:1:4ff::/64
		3 (1000)	2001:db8:1:800::/56	2001:db8:1:800::/64 to 2001:db8:1:8ff::/64
2 (0100)	2001:db8:1:4000::/52	1 (0000)	2001:db8:1:4000::/56	2001:db8:1:4000::/64 to 2001:db8:1:40ff::/64
		1 (0001)	2001:db8:1:4100::/56	2001:db8:1:4100::/64 to 2001:db8:1:41ff::/64
		2 (0100)	2001:db8:1:4400::/56	2001:db8:1:4400::/64 to 2001:db8:1:44ff::/64
		3 (1000)	2001:db8:1:4800::/56	2001:db8:1:4800::/64 to 2001:db8:1:48ff::/64
3 (1000)	2001:db8:1:8000::/52	1 (0000)	2001:db8:1:8000::/56	2001:db8:1:8000::/64 to 2001:db8:1:80ff::/64
		2 (0100)	2001:db8:1:8400::/56	2001:db8:1:8400::/64 to 2001:db8:1:84ff::/64
		3 (1000)	2001:db8:1:8800::/56	2001:db8:1:8800::/64 to 2001:db8:1:88ff::/64
4 (1100)	2001:db8:1:c000::/52	1 (0000)	2001:db8:1:c000::/56	2001:db8:1:c000::/64 to 2001:db8:1:c0ff::/64
		2 (0100)	2001:db8:1:c400::/56	2001:db8:1:c400::/64 to 2001:db8:1:c4ff::/64
		3 (1000)	2001:db8:1:c800::/56	2001:db8:1:c800::/64 to 2001:db8:1:c8ff::/64

Fuente: CISCO, 2008.

4. Longitud de Subredes

Existen dos escenarios a considerar cuando se trata de los prefijos de segmentos de red: las estaciones final y segmentos de infraestructura. Para los segmentos que tienen estaciones finales conectadas a ellas, el direccionamiento RFC para IPv6 sugieren que un /64 puede utilizar la longitud del prefijo. Es poco probable que, con 264 direcciones disponibles por segmento, se vean longitudes de prefijo más corto que /64 para los segmentos host finales; también se requiere un prefijo /64 si la autoconfiguración sin estado va a ser utilizado para asignar el ID de interfaz a las estaciones finales.

De igual manera, hay muchas opciones disponibles en la asignación de prefijos para la infraestructura de red. Los planificadores de redes optan a ser consistente a través de la red y desplegar prefijos /64 para la infraestructura de red y para la sede de segmentos de acceso; además pueden optar por un plan que utiliza longitudes de prefijo mayores que /64. Por consiguiente, teniendo estas opciones disponibles, no hay reglas duras y rápidas para la asignación de prefijos. Es en esta etapa donde el plan de direccionamiento de redes debe considerar los principios mencionados más arriba: la planificación, la agregación y el crecimiento. La Tabla 8 expone algunas pautas que se deben considerar al asignar prefijos a un enlace.

Tabla 8
Consideraciones a nivel de prefijos

64 Bits	< 64 Bits	> 64 Bits
Recomendado por el RFC 3177 e IAB / IESG	Permite más *hosts* por subred	La conservación de espacio de direcciones
La consistencia hace facilidad de gestión	Considerada mala práctica	Complica la gestión
Subred no alineada con el número final de sistemas, perciben "residuos" de espacio de direcciones	64 bits ofrece más espacio para hosts que el tipo actual y puede transportar de manera eficiente	Debe evitar la superposición con direcciones específicas: - *Router Anycast* (RFC 3513)- RP *Embedded* (RFC 3956)- Direcciones ISATAP

Fuente: CISCO, 2008.

Por otro lado, existen problemas potenciales cuando se considera el uso de prefijos mayores que /64. Una primera preocupación tiene que ver con las posiciones de *bits* 71 y 72 ("u" y "g" bits cada uno) en la dirección IPv6; estos *bits* tienen un significado determinado y su valor debe establecerse como es debido. El *bit* 71 identifica si la dirección es única a nivel mundial o asignado en el lugar y el bit 72 identifica si la dirección es *unicast* o *multicast*. Otra consideración al utilizar prefijos mayores a /64 tiene que ver con las direcciones *anycast*, debido a que la planificación de la red debe evitar el uso de un identificador interfaz todos cero, definido por el RFC 4291 como la dirección *anycast* subred del *router*. La otra dirección de difusión por proximidad a evitar es la reservada subred *anycast* IPv6 (dirección definida en el RFC 2526), en donde los últimos siete bits están reservados para el ID de difusión por proximidad y los otros bits del identificador se ponen a 1.

Otra área de preocupación tiene que ver con las direcciones del Intra Site Automatic Tunnel Address Protocol –ISATAP–, las cuales requieren /64 para su uso e incrustan la dirección IPv4 en los últimos 32 *bits* de la dirección IPv6. Para completar el identificador de interfaz de host, ISATAP utiliza 0000: 5efe; sin embargo, esta frecuencia debe evitarse cuando se consideran prefijos de longitudes mayores a /64. Un enfoque recomendado para la infraestructura de la red seria implementar prefijos /64, /126 y /128, siendo este último utilizado para las direcciones de bucle invertido para identificar nodos de la red; mientras que los prefijos /65 o /126 son utilizados para enlaces punto a punto, como los enlaces de serie o de punto de final. Por consiguiente, un esquema /64 es el más simple de implementar y un esquema de prefijo /126 permite la conservación de la mayoría de las direcciones.

Es necesario mencionar que se utilizan cuatro bits para identificar la región, cuatro *bits* para identificar un sitio dentro de una región y cuatro bits por sitio. La Tabla 9 muestra cómo se podría implementar el esquema /64.

Tabla 9
Despliegue de la Infraestructura del Prefijo /64

Infrastructure prefix— 2001:db8:1:e000::/51				
Region (4 bits)	Regional Prefix	Facility (4 bits)	Facility prefix	Subnets per facility (4 bits)
1 (0000) (0001)	2001:db8:1:c000::/56	1 (0000) (0001)	2001:db8:1:c000::/59	2001:db8:1:c000::/64 to 2001:db8:1:c01f::/64
		2 (0100) (0101)	2001:db8:1:e040::/59	2001:db8:1:e040::/64 to 2001:db8:1:e05f::/64
		3 (1000) (1001)	2001:db8:1:e080::/59	2001:db8:1:e080::/64 to 2001:db8:1:e09f::/64
2 (0100)	2001:db8:1:e400::/56	1 (0000) (0001)	2001:db8:1:e400::/59	2001:db8:1:e400::/64 to 2001:db8:1:e41f::/64
		1 (0010) (0011)	2001:db8:1:e420::/59	2001:db8:1:e420::/64 to 2001:db8:1:e41f::/64
		2 (0100) (0101)	2001:db8:1:e440::/59	2001:db8:1:e440::/64 to 2001:db8:1:e44f::/64
		3 (1000) (1001)	2001:db8:1:e480::/59	2001:db8:1:e480::/64 to 2001:db8:1:e48f::/64
3 (1000)	2001:db8:1:f800::/56	1 (0000) (0001)	2001:db8:1:f800::/59	2001:db8:1:f800::/64 to 2001:db8:1:f81f::/64
		2 (0100) (0101)	2001:db8:1:f840::/59	2001:db8:1:f840::/64 to 2001:db8:1:f85f::/64
		3 (1000) (1001)	2001:db8:1:f880::/59	2001:db8:1:f880::/64 to 2001:db8:1:f89f::/64
4 (1100)	2001:db8:1:fc00::/56	1 (0000) (0001)	2001:db8:1:fc00::/59	2001:db8:1:fc00::/64 to 2001:db8:1:fc1f::/64
		2 (0100) (0101)	2001:db8:1:fc40::/59	2001:db8:1:fc40::/64 to 2001:db8:1:fc5f::/64
		3 (1000) (1001)	2001:db8:1:fc80::/59	2001:db8:1:fc80::/64 to 2001:db8:1:fc9f::/64

Fuente: cisco, 2008.

Mientras que una implementación alternativa es usar /126 donde cuatro bits se utilizan para identificar la región y cuatro bits se utilizan para identificar el sitio. Este esquema le da a cada sitio 254 subredes de infraestructura. La Tabla 10 muestra cómo se podría implementar este esquema.

Tabla 10
Despliegue de la infraestructura del prefijo /126

Infrastructure prefix - 2001:db8:1:ffff::/64				
Region (4 bits)	Regional Prefix	Facility (4 bits)	Facility prefix	Subnets per facility (54 bits)
1 (0000) (0001)	2001:db8:1:ffff:0::/68	1 (0000)	2001:db8:1:ffff:0::/72	2001:db8:1:ffff::/126 to 2001:db8:1:ffff:00ff:ffff:ffff:fffc::/126
		2 (0100)	2001:db8:1:ffff:0400::/72	2001:db8:1:ffff:0400::/126 to 2001:db8:1:ffff:04ff:ffff:ffff:fffc::/126
		3 (1000)	2001:db8:1:ffff:0800::/72	2001:db8:1:ffff:0800::/126 to 2001:db8:1:ffff:08ff:ffff:ffff:fffc::/126
2 (0100)	2001:db8:1:ffff:4000:/68	1 (0000)	2001:db8:1:ffff:4000::/72	2001:db8:1:ffff:4000::/126 to 2001:db8:1:ffff:40ff:ffff:ffff:fffc::/126
		2 (0100)	2001:db8:1:ffff:4400::/72	2001:db8:1:ffff:4200::/126 to 2001:db8:1:ffff:42ff:ffff:ffff:fffc::/126
		3 (1000)	2001:db8:1:ffff:4800::/72	2001:db8:1:ffff:4400::/126 to 2001:db8:1:ffff:44ff:ffff:ffff:fffc::/126
3 (1000)	2001:db8:1:ffff:8000:/68	1 (0000)	2001:db8:1:ffff:8000::/72	2001:db8:1:ffff:8000::/126 to 2001:db8:1:ffff:80ff:ffff:ffff:fffc::/126
		2 (0100)	2001:db8:1:ffff:8200::/72	2001:db8:1:ffff:8400::/126 to 2001:db8:1:ffff:84ff:ffff:ffff:fffc::/126
		3 (1000)	2001:db8:1:ffff:8400::/72	2001:db8:1:ffff:8800::/126 to 2001:db8:1:ffff:88ff:ffff:ffff:fffc::/126
4 (1100)	2001:db8:1:ffff:c000:/68	1 (0000)	2001:db8:1:ffff:c000::/72	2001:db8:1:ffff:c000::/126 to 2001:db8:1:ffff:c0ff:ffff:ffff:fffc::/126
		2 (0100)	2001:db8:1:ffff:c400::/72	2001:db8:1:ffff:c400::/126 to 2001:db8:1:ffff:c4ff:ffff:ffff:fffc::/126
		3 (1000)	2001:db8:1:ffff:c800::/72	2001:db8:1:ffff:c800::/126 to 2001:db8:1:ffff:c8ff:ffff:ffff:fffc::/126

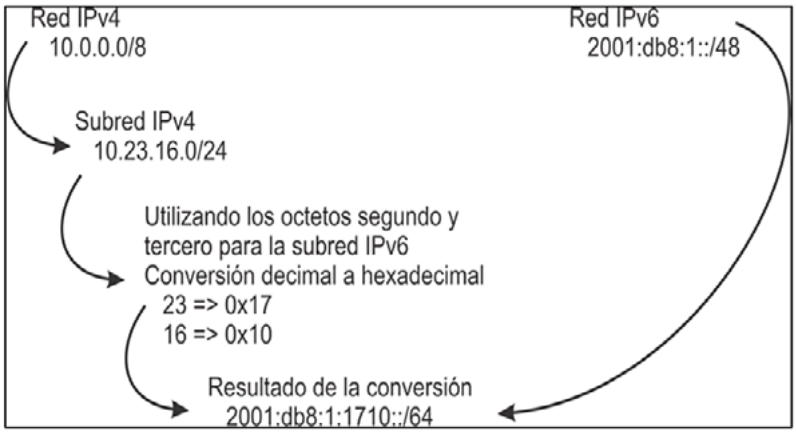
Fuente: CISCO, 2008.

E. Implementación del plan de direcciones

Los métodos disponibles para desarrollar el plan de direccionamiento IPv6 son los siguientes:

a) Basado en IPv4 existente que se traduce en IPv6

Figura 22
Conversión IPv4 a IPv6



Fuente: CISCO, 2008.

b) Basado topológicamente

Este método asigna un bloque de direcciones a todos los nodos dentro de las limitaciones topológicas de la red. Por ejemplo, a un cliente se le ha asignado el 2001:DB8: 1: /48 de su proveedor y tienen sitios en todo el país que están de forma topológica dividido en cuatro regiones por geografía; se podría optar por utilizar los primeros cuatro bits, de los 16 *bits* que tiene para subredes, para identificar cada región. Con este esquema de la red podría tener dieciséis regiones y cada región puede tener 4096 (212) /64 subredes. Este esquema podría ir más lejos si el cliente opta por utilizar los últimos cuatro *bits* para identificar una instalación dentro de cada región, lo que permitiría 16 sitios (24) por región, en cada sitio posible 256 (28) /64 subredes.

c) Basado Organizacionalmente

Implica la asignación de prefijos basados en límites de la organización dentro de un cliente. En este caso, el área de ingeniería recibe un bloque de direcciones, el área de ventas un diferente bloque, área legal otro bloque, y así cada vez. Un problema importante con este método es que no promueve un esquema de agregación eficiente. Es probable

que la mayoría de las áreas dentro de una empresa se encuentren en múltiples sitios debido a esta dispersión organizativa; además de la probabilidad de que este esquema se use en conjunción con un despliegue topológico.

d) Basado en Servicios

Consiste en asignar prefijos basados en el tipo de servicio que se ofrece como los dispositivos que proporcionan VolP o servicios inalámbricos. Este método tiene los mismos problemas de agregación como el basado en la organización; también es probable que se use este esquema en conjunción con el despliegue topológico.

F. Asignación de Identificadores de Interfaz

Por último, otra consideración a la hora de desarrollar el plan de direccionamiento es cómo se asigna el identificador de interfaz a las estaciones e infraestructura de red a terminar. RFC 5.157 tiene algunas recomendaciones relacionadas con la asignación de direcciones y las implicaciones relacionadas con la subred de exploración. Hay varias opciones de asignación de identificadores de interfaz: manual, sin estado, extensiones de privacidad, SEND/CGA y DHCP.

III. Transición de IPv4 a IPv6

El IPv6 se origina a raíz del planteamiento del agotamiento de casi 4.300 millones de direcciones IPv4 de 32 bits, ofreciendo una cantidad infinita de direcciones únicas de 128 bits. Otras ventajas que presenta el IPv6 son: mayor rendimiento debido a la eficiencia del *routing* y al *multicasting* de calidad superior, así como mayor velocidad en las transacciones por redes VPN; mayor seguridad con el empleo obligatorio de IP Security –IPsec–; mejor compatibilidad con los dispositivos móviles y calidad de servicio optimiza el rendimiento de transmisiones.

Las consideraciones que se deben tener en cuenta al implementar el IPv4 son las siguientes:

- **Verificar la conectividad de subida**: Se debe consultar a los proveedores de servicios de Internet –ISP– sobre cómo admitirá los estándares IPv4 e IPv6 y cuál es su plazo.
- **Controlar los equipos IPv4:** Para determinar todos los equipos que aun funcionan con el IPv4 o que admiten ya el IPv6.
- **Realizar una auditoría de sistemas operativos y aplicaciones:** Esto determina si están habilitados o ya necesitaran el estándar IPv6.

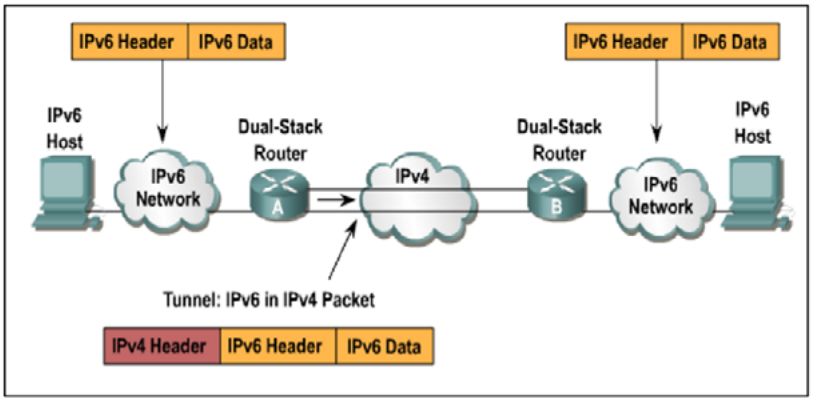
Por otro lado, las consideraciones que deben tomar a la hora de implementar el IPv6 son las siguientes:

- Elaborar y aplicar las conversiones.
- Utilizar tecnología de doble pila juntar los sistemas del Ipv4 e IPv6 en la red.
- Aplicar un modelo de transición para conectarse, a través de la tecnología de doble pila, a las direcciones IPv6 por una red IPv4.
- Utilizar las aplicaciones de traducción para conectar a los usuarios IPv6 que quieren tener acceso al IPv4 en Internet.
- Incorporar la seguridad en IPv6.
- Aplicar la tecnología de forma gradual y con pruebas, se mantenienen informados, se solicitan opiniones a los usuarios y se analizan las estadísticas operativas.
- Supervisar, registrar y comunicar todos los procesos, efectos y consecuencias que trae la transición de IPv4 a IPv6 de la empresa.

A. VPN Túnel

El propósito de todos los proveedores de Internet es que todo sea IPv6; sin embargo, aún se da una transición lenta y gradual en donde ciertas partes del Internet solo funcionarán en IPv4 o, también, que algunos nodos claves dentro del Internet no pueden realizar la transición a IPv6; por lo que se tiene que dar soluciones temporales en ambos casos. La solución más habitual que se ha originado son los túneles. La Figura 23 muestra un escenario donde los túneles son utilizados.

Figura 23
Túneles



Fuente: CISCO, 2010.

– Túnel en una Red

Un túnel se caracteriza por modificar el encabezado original de IPv6, el cual se convierte en parte de los datos de un nuevo protocolo, en este caso el IPv4, y dicho puerto destino reconoce el método del túnel empleado. El protocolo IPv6, convertido ahora en datos de un protocolo IPv4, se desplazará por la red en este nuevo formato hasta llegar a un destino que, por medio de los puertos involucrados, identifique el túnel y retire el encabezado de IPv4 para pasarlo a una red IPv6. Para ello, es necesario que los enrutadores perimetrales a los tramos de IPv4 e IPv6 sean capaces de soportar *dual-stack*.

– Túnel Manual

Es la configuración que utilizará la relación de direcciones IPv4 con IPv6 de manera estática y sólo podrá transportar paquetes de IPv6 a islas establecidas hasta ahora. Este método es el que permite comunicar las partes internas de un sitio –LAN– o intercomunicar dos sitios cuando el camino no radica en IPv6.

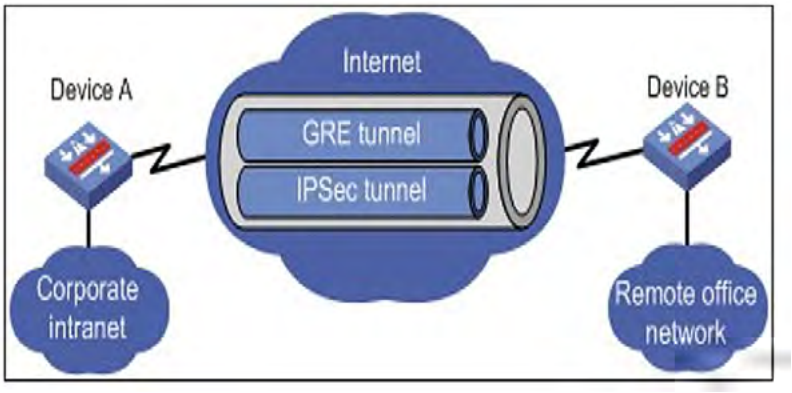
– Generic Routing Encapsulation –GRE–

El GRE permite que los túneles puedan ser seguros, pero posee desventaja similar al método manual en el aspecto de que cada enlace (túnel) debe ser con anterioridad configurado y no es posible determinar si en el enlace se encuentra disponible. Dado esto, la GRE cuenta con métodos de "keep-alive" para mantener el estatus de la red; esto no soluciona los problemas, pero valida el estado del túnel. Del mismo modo, GRE suele ser el túnel por defecto en los enrutadores de la marca Cisco, por lo tanto, si el usuario no especifica un protocolo, será el protocolo GRE el que actúe.

En la Figura 27 se visualiza que GRE puede trabajar con IPsec, permitiendo que los paquetes de datos como el protocolo de enrutamiento, voz y paquetes de video a encapsular por GRE sean codificadas por IPsec para mejorar la seguridad de la transmisión de datos en un túnel.

Figura 24

GRE



Fuente: CISCO, 2010.

B. Infraestructura de Claves Públicas –PKI–

Una Infraestructura de Claves Públicas –PKI– se caracteriza por ser un conjunto de *software*, *hardware*, usuarios y procedimientos que son necesarios para originar, gestionar, almacenar, distribuir y revocar certificados de clave pública. De la misma manera, puede proporcionar

la gestión de certificados de clave pública y privada confiable y eficiente, permitiendo el uso de la autenticación y servicios de seguridad confidenciales; para proporcionar estos servicios, una PKI utiliza sus componentes básicos, que incluyen un servicio de certificación, una autoridad de registro y un servidor de petición. Algunas PKI utilizan componentes adicionales, dependiendo de los servicios que sus implementaciones particulares ofrecen. Por otro lado, el PKI ofrece, a nivel de aplicación, a los protocolos de red IPv6 los siguientes factores:

- Proporcionar acceso directo y autóctono a través de una red de sólo IPv6 o *dual stack* a través de Internet a todos los servicios PKI. Las entidades finales, los usuarios y los procesos utilizan estos servicios para generar y administrar su información criptográfica; cabe destacar que IPv6 es una de las mejores respuestas de la comunidad científica a los desafíos presentados por el crecimiento continuo de Internet, que requiere arquitecturas evolutivas para adaptarse a las nuevas tecnologías que apoyan un creciente número de usuarios, aplicaciones y servicios.
- Permitir y promover servicios y aplicaciones relacionadas con la seguridad en una red IPv6 o dual stack, redes VPN, servidores web seguros y AAA (Autenticación, Autorización y Auditoría) que son comunes en las arquitecturas de comunicación y entornos de aplicaciones distribuidas; además de utilizar la información de clave pública para proteger comunicaciones. En consecuencia, se benefician de la eficiencia y escalabilidad con el uso de IPv6 como la capa de red. Eficiencia y escalabilidad son dos de las características principales de IPv6 frente a IPv4.
- Los servicios y dispositivos que, a través de la Red Privada Virtual –VPN– de IPv6, ofrecen puntos finales virtuales seguros a su dirección IPv6 que incluye los certificados X.509 públicos para establecer comunicaciones seguras. Es necesario señalar que sólo una PKI IPv6 puede generar y gestionar dichos certificados.

1. Log de Auditoría

El alcance de la auditoría PKI y el mecanismo de presentación de informes dependerán de los objetivos de la auditoría y los destinatarios de los informes. En algunos casos, la auditoría se realiza para fines internos, para proporcionar información a la dirección sobre la calidad del diseño de la PKI y la eficacia operativa de los controles o para satisfacer los requisitos de auditoría interna. En otros casos, se lleva a cabo la auditoría para ejecutar todas las necesidades de las partes externas, tales como clientes, reguladores y autoridades políticas para los entornos de confianza. En la mayoría de los casos, la auditoría se puede realizar por una combinación de efectos internos y externos.

El alcance de una auditoria PKI general debe incluir cuatro áreas de auditoría que son controlados por la Autoridad Certificadora –CA–, las cuales son:

- Prácticas Comerciales de Divulgación (gestión y documentación de políticas): son los requisitos de la CA para los tipos o clases de certificados, sus prácticas específicas para el funcionamiento de la CA y la forma en que la organización informa a los usuarios finales y/o terceros en relación con sus políticas y prácticas.
- Controles Ambientales (gestión de TI en general): los procesos, políticas, procedimientos y controles técnicos crean un entorno seguro y de confianza para la CA.
- Gestión del Ciclo de Vida Clave: son los procedimientos y controles técnicos para conservar la seguridad e integridad de claves de CA a través de sus ciclos de vida.
- Certificado de Gestión de Ciclo de Vida: son los procedimientos y controles técnicos relativos a la gestión de los certificados a través de sus ciclos de vida.

Por otro lado, existen tres fases principales de una auditoría de PKI:

– Planificación

Permite al auditor comunicar el plan global de auditoría a la CA y confirmar un entendimiento común del enfoque de auditoría. Además, esta fase proporciona a la CA una compresión de los procesos de auditoria y permite prepararse para la auditoría. Esta fase de planificación es necesaria para asegurar que todos los usuarios que participan en el proceso de auditoría tienen un entendimiento común de las metas y objetivos de la auditoria.

– Ejecución

En esta fase se llevan a cabo los procedimientos de prueba. Al evaluar el diseño, la auditoria se centrará en la integridad y suficiencia de procesos, políticas, procedimientos de la CA y el diseño de la arquitectura PKI. Además de la revisión de la documentación y entrevistas, este proceso incluye la prueba específica realizada de forma selectiva en los controles críticos. De esta manera, si la auditoría abarca un periodo de tiempo, los procedimientos de prueba deben realizarse para comprobar la efectividad operativa de los controlas de la CA durante el periodo cubierto por el informe de auditoría. Estos procedimientos de prueba adicionales incluyen investigaciones que confirmarán la inspección de la documentación que acredite que los procedimientos operativos se siguen con exactitud, la revisión de las configuraciones del sistema (por ejemplo, sistemas de CA, base de datos, directorios, sistemas operativos, *firewalls*, *routers*, etc.), la observación de los procesos y controles clave, retroalimentación de determinados procesos, y otros tipos de procedimientos de prueba.

– Presentación de informes

Al finalizar la fase de ejecución, se prepara el informe de auditoría PKI; el tipo específico de informe dependerá de los objetivos de la auditoría y se define en la etapa de planificación. Si se prepara el informe para fines en exclusiva internos toma la forma de un informe de evaluación de riesgos PKI; en cambio, si el informe es para propósitos externos, podría tomar la forma de un WebTrust, una declaración de terceros, un

informe SAS 70, o de otra forma adecuada. Junto con el informe externo, el auditor por lo general se prepara una carta de gestión que ofrece recomendaciones para mejorar el diseño y las operaciones de PKI.

2. Procedimientos

En muchos países, la supervisión de PKI y/o sistemas de acreditación han sido o están siendo establecidas. Por ejemplo, se estableció la Directiva Europea sobre la firma electrónica para estimular el comercio, facilitar su uso y aportar su reconocimiento jurídico en todos los Estados miembros de la UE a través del uso de certificados reconocidos que cumplan determinados criterios. En apoyo de la directiva, el Reino Unido y los Países Bajos han establecido sistemas voluntarios de acreditación por el que una CA, proveedor de servicios de cifrado –CSP–, puede ser certificada para emitir certificados reconocidos. Este tipo de certificación se basa en los estándares técnicos como X9.79 y WebTrust para las CA y puede proporcionar estatus legal mejorado para firmas digitales mediante certificados reconocidos. En otros países, como Estados Unidos, algunos estados han establecido requisitos de licencia por el que una CA con licencia puede obtener la aprobación para hacer negocios con el gobierno estatal o alcanzar un determinado estatuto jurídico para la firma digital mediante certificados emitidos por la entidad emisora con licencia.

3. Marco Legal

Existen una serie de normas nacionales e internacionales que se han desarrollado para ayudar a los auditores e implementadores de PKI. Estándares de PKI se pueden aprovechar para proporcionar una base consistente para la auditoría de los controles a través de entidades emisoras de certificados PKI, mejorar la calidad de una implementación PKI, aumentar la eficiencia de las operaciones y ayudar a permitir la interoperabilidad con otras PKI. Una de las normas más conocidas y aprobadas para las operaciones de CA es la Norma Nacional Americana –ANS– X9.79: 2000. PKI Prácticas y Políticas de Framework. X9.79 in-

cluye criterios de control de CA que se basaban en el cuerpo existente de normas internacionales (ISO, IETF, BSI) y Estados Unidos (ANSI, FIPS, ABA) vinculado a las gestiones de certificados, de claves y de seguridad. Luego, el Grupo de Trabajo de Comercio de Garantía de AICPA / CICA Electronic adoptó los criterios X9.79 como base del programa WebTrust para Autoridades de Certificación (WebTrust para las CA), que proporciona un marco de auditoría diseñado en específico para las CA y ha sido adoptado por las organizaciones profesionales de contabilidad en más de 15 países. Además, la Organización Internacional de Normalización –ISO– en la actualidad se desarrolla un estándar internacionalizado (ISO 21188) para las prácticas de PKI se utiliza X9.79 como entrada principal.

Por otra parte, el X9.79 y WebTrust para criterios CAs continúan ganando amplia adopción internacional. Por ejemplo, estos criterios han sido:

- Aprobados por Microsoft como una exigencia de certificados de CA raíz que se incluirán en los navegadores de Microsoft.
- Reflejados en el Instituto Europeo de Normas de Telecomunicaciones –ETSI– como un apoyo técnico de la Directiva Europea de Firma Electrónica de 1999.
- Reflejados en el cumplimiento Identrus y controles Directrices para la evaluación.
- Avalados por el Foro PKI.
- Referenciados por la American Bar Association –ABA– en sus directrices de evaluación de PKI.
- Dentro de las PKI individuales o comunidades cerradas, las normas específicas a menudo se especifican. En algunos casos éstos se derivan de las normas existentes, mientras que en otros se establecen requisitos diferentes.

IV. Visión global sobre los tipos de desastres

A nivel global y general, en los países de América del Sur pueden ocurrir diversos tipos de desastres definidos como desastres naturales y desastres antrópicos.

A. Desastre Natural

Los desastres naturales, a su vez, están divididos como desastres de fenómenos de geodinámica interna, fenómenos de geodinámicas externas y fenómenos hidrometeorológicos.

B. Fenómenos de Geodinámica Interna

– Sismos

Son sucesos que no se sabe cuándo vendrán y que son recurrentes, pero se sabe que llegarán y por eso es necesario aplicar una cultura de prevención contra los sismos, debido a las consecuencias que puede traer esto como la mortalidad, la debacle económica y la devastación de las áreas naturales. En este caso, se hablará de Perú como un país que está ubicado en la zona central y occidente de Suramérica, dentro de lo que se conoce como el Cinturón de Fuego del Pacífico, zona propensa a que ocurran el 85% de los eventos sísmicos y se enciendan los volcanes. Del mismo modo, tiene al frente de su costa la Placa de Nazca, en donde se originan fuga de energía que provocan los movimientos telúricos al interactuar con la Placa Continental o Sudamericana. Por otro lado, se puede encontrar que además de ser movimientos de poca o gran magnitud e intensidad, también la población no está capacitada y preparada para defenderse a la hora de algún sismo, al provocar que las consecuencias sean del todo devastadores.

– Tsunamis

Son aquellos fenómenos que ocurren a nivel del mar, son pocos frecuentes, pero de gran magnitud al ser una sucesión de olas con gran altura que se acercan a las costas de manera gradual lo que ocasiona destrucción y pérdidas humanas. Esto se origina, en su mayor parte, a causa de: movimientos telúricos de gran magnitud con epicentros en el fondo del océano o cercado a él, erupciones volcánicas cerca de las costas o por derrumbes de fondos marinos. De esta manera, no existe una defensa eficaz contra estos desastres, sin embargo, es necesario la organización

y la preparación con un sistema de alerta eficaz y accesible para todas las personas que indique el momento en que se debe evacuar y dirigirse a un refugio de seguridad que esté lejos de las costas o en partes altas, permitiendo controlar y menguar las consecuencias devastadoras.

C. Fenómenos de Geodinámica Externa

– Flujo de Huaycos o Flujo Aluviónico

Son flujos de una mezcla de agua y grandes proporciones de sólidos, constituyendo lodos; producen graves daños por su gran masa y velocidad. En Perú, los huaycos en la región Ica son gigantescos y, debido a la masa que transportan, tienen una gran fuerza y caudal superior al río Ica; estos huaycos no son de agua limpia, sino corrientes de barro espesas, sobre las cuales se arrastran rocas de hasta 40 toneladas de peso. De esta manera, los terrenos en los conos no deben ser habitados y las corrientes de barro no deben ser encauzadas hacia el río Ica ya que podrían ser desbordados.

D. Fenómenos Hidrometereológico

– Inundaciones

Son los desbordes del río que están asociados al flujo de huaycos y constituyen problemas climáticos y recurrentes de la zona en que ocurra. En la actualidad, son muchas zonas y personas afectadas por estos fenómenos, al causar grandes devastaciones en la comunidad. En Perú, por ejemplo, las personas de escasos recursos son los que siempre se asientan en las zonas de alto riesgo de inundación.

E. Desastres Antrópicos

Son aquellos desastres que son producidos por la mano de obra y actividad del hombre y que, además, generan desastres de grandes proporciones en cualquier momento, al provocar eventos de emergencia

sorpresiva o pequeños daños en muchas ocasiones que se acumulan y desencadenan peligros considerables. Algunos de los efectos de las actividades humanas que forman amenazas para la seguridad son: el efecto invernadero, la desforestación, la contaminación ambiental, los accidentes químicos, los materiales erosivos, el terrorismo, la alteración de procesos naturales y los incendios provocados. En este contexto, se identificarán y analizarán los niveles peligrosos de la contaminación ambiental y de las sustancias químicas en base a una escala cuantitativa y descriptiva desde cero como un peligro nulo hasta uno como un peligro elevado.

– Niveles de peligro de inflamabilidad

- *Grado 4*: materiales que se vaporizan de manera rápida y por completo a la temperatura y presión atmosférica ambiental, o que se dispersan o se queman con rapidez en el aire. Incluye: gases, sustancias criogénicas, cualquier material líquido o gaseoso, materiales que forman mezclas explosivas con el aire y que se dispersan sin demora tales como el polvo de combustible sólido y vapor de las gotas o lloviznas de líquidos inflamables o combustibles.
- *Grado 3*: materiales líquidos que pueden encenderse en casi todas las condiciones de temperatura ambiental. Estos materiales producen una atmósfera peligrosa con el aire en casi todas las temperaturas ambientales, y aunque ésta no los afecta, se producen aprisa en casi cualquier condición. Incluye: líquidos con un punto de inflamación por debajo o por encima de 73° F o 22° C y con un punto de ebullición superior o inferior a 100° F o 37° C, líquidos inflamables clase 1B y 1S, materiales sólidos en forma de polvo, materiales fibrosos o tejidos que se queman de inmediato, materiales que arden con extrema rapidez por su contenido de oxígeno, materiales que se pueden quemar desde luego al contacto con el aire.
- *Grado 2*: materiales que deben calentarse un tanto o exponerse a temperaturas altas antes de que ocurra la ignición; no forman atmósferas peligrosas con el aire en condiciones normales, pero bajo temperaturas ambientales altas o calor mode-

rado pueden liberar vapor en cantidades suficientes capaces de producir atmósferas peligrosas con el aire. Incluye: líquidos combustibles que tienen un punto de inflamación por encima de los 100° F o 37° C, pero sin exceder 200° F o 93,4° C.
- *Grado 1*: materiales que deben precalentarse antes que la ignición ocurra; requieren un pre calentamiento considerable en todas las condiciones de temperaturas ambientales, antes de que la ignición y la combustión tengan lugar. Incluye: materiales que arden en el aire al exponerse por un periodo de cinco minutos, sólidos y semisólidos que tienen un punto de inflamación por encima de 200° F o 93.4° C, la mayoría de los materiales combustibles.
- *Grado 0*: materiales que no se queman. Incluye cualquier material que no se quema en el aire cuando se expone por un período de cinco minutos a temperatura de 15° F o 4° C.

– Niveles de peligro de toxicidad

- *Grado 4*: sustancias que, con sólo una corta exposición, pueden causar la muerte o daño permanente que requiera de atención médica inmediata; son materiales peligrosos que requiere de un equipo especial de protección. Incluye: materiales que pueden traspasar los trajes encapsulados contra incendios protegidos con caucho común, materiales que liberan gases que son en extremo peligrosos, tóxicos o corrosivos al tener contacto o al inhalarse; materiales que liberan productos de combustión muy tóxicos; materiales que son corrosivos para los tejidos vivos o tóxicos por la absorción de la piel.
- *Grado 3*: sustancias que pueden causar incapacidad temporal o posibles daños permanentes aun cuando se proporcione tratamiento médico. Incluye: materiales que liberan productos tóxicos combustibles, materiales que liberan productos combustibles muy irritantes, materiales que liberan vapores tóxicos que no se puedan detectar.
- *Grado 2*: sustancias que pueden causar incapacidad temporal o posible daños permanentes a menos que se proporcione tratamiento médico inmediato. Incluye: materiales que liberan

productos tóxicos combustibles, materiales que liberan productos combustibles muy irritantes, materiales que liberan vapores tóxicos que no se puedan detectar.
- *Grado 1*: sustancias que, bajo exposición natural, causan irritaciones o daños residuales menores en ausencia de tratamiento médico. Incluye: materiales que liberan productos de combustión irritante, materiales que producen irritaciones en la piel sin dañar el tejido.
- Grado 0: sustancias que no ofrecen otro peligro que el del material combustible ordinario.

– Niveles de peligro de reactividad

- *Grado 4*: materiales que son capaces de explotar por sí mismos con reacciones explosivas a temperaturas y presión normales. Incluye materiales que son susceptibles a golpes térmicos o mecánicos a temperaturas y presiones normales.
- *Grado 3*: materiales que son susceptibles de detonación o de descomposición explosivas que requiere de un fuerte agente iniciador o que deban calentarse antes de la ignición. Incluye materiales que son susceptibles a golpe mecánico, térmico a temperatura y presión elevadas o que reaccionan con agua sin necesidad de calor o confinamiento.
- *Grado 2:* materiales inestables que están listos a sufrir cambios químicos violentos pero que no detonan. Incluye: materiales que pueden sufrir cambios químicos con liberación rápida de energía a normal temperatura y presión, y que pueden sufrir cambios violentos a temperaturas y presiones elevadas; materiales que reaccionan de manera violenta al contacto con el agua o que pueden formar mezclas en potencia explosivas con el agua.
- *Grado 1*: materiales que son por lo común estables, pero que, sometidos a elevadas temperaturas y presiones, pueden llegar a ser inestables o que pueden reaccionar, de forma no violenta, al contacto con el agua o con alguna liberación de energía.
- *Grado 0*: materiales que son por lo general estables aún en condiciones de incendio y que no reaccionan con el agua.

Capítulo cuarto
Estudios sobre la implementación de controles de seguridad para recuperar datos en caso de desastre a través del protocolo IPv6

La Informática empresarial es vital para la estabilidad y éxito de las actividades que son desarrolladas en una organización, de manera que puedan tener la capacidad de prevenir un posible impacto de menor o mayor gravedad en los sistemas tecnológicos y en la central de datos y así poder reanudar las actividades sin ninguna pérdida de información ni de aplicación, manteniendo el funcionamiento y la operatividad de los equipos, de los sistemas y de la información que se maneja dentro de la organización. En el mundo tecnológico, hoy por hoy, todas las operaciones y actividades de una empresa u organización están propensas a cualquier interrupción, lo que preocupa a la comunidad debido al aumento de amenazas hacia las empresas y organizaciones y origina así, que se busquen posibles soluciones al respecto. Es a causa de esto, que se propone en este trabajo investigativo el desarrollo e implementación de un Plan de Recuperación de Datos en caso de desastre, ya sea natural o de cualquier otra índole.

Al desarrollar e implementar un Plan de Recuperación de Datos en caso de desastre, las empresas obtienen grandes e importantes beneficios como pueden ser: el cese de riesgos al afrontar y minimizar las potenciales pérdidas de las actividades u operaciones críticas que se desarrollan dentro de ella; la identificación de los sistemas vulnerables y críticos que posee la empresa; la posibilidad de reanudación de actividades y de recuperación de información a corto plazo; la protección de los activos y las responsabilidades legales de la empresa; el cese de los errores humanos por estrés ante un desastre; la elaboración de material de entrenamiento y capacitación para todo el personal.

En ese sentido, el objeto del estudio denominado Servicio Nacional de Adiestramiento en Trabajo Industrial –SENATI– zonal Sur, ubicado en la región Ica de Perú, es una institución de formación y capacitación profesional creada a iniciativa de la Sociedad Nacional de Industrias en 1961, y se caracteriza por diseñar y desarrollar programas de formación en respuesta a la demanda de calificación para el trabajo de las actividades económicas.

Es importante acotar que SENATI cuenta con un número muy limitado de especialistas en los temas de seguridad informática. Si bien existe un buen número de profesionales con experiencia en estos temas, apenas ninguno de ellos ha recibido especializaciones vinculadas al diseño y ejecución de programas para crear y consolidar un Plan de Recuperación de Datos en caso de Desastres; siendo un tema muy importante debido a que sus ideas han ido evolucionado muy rápido durante los últimos años y con las actualizaciones tecnológicas. De esta manera, se puede decir que no contar con un plan ante la potencial pérdida de información puede acarrear importantes pérdidas económicas, tal como se muestra en las Tablas 11 y 12.

Tabla 11
Ingresos y Egresos SENATI - Ica 2017

EGRESOS	ENERO	FEBRERO	MARZO
60 Compras	0.00	0.00	0.00
62 Personal de instrucción	6,695.00	6,695.00	6,695.00
Supervisión directa jefe CFP (5%)	334.75	334.75	334.75
63 Servicio de Energía Eléctrica	220.00	180.00	170.00
63 Servicio de Telefonía	204.00	204.00	204.00
63 Servicio de Agua Potable	71.30	71.30	71.30
63 Servicio de Limpieza	1,251.00	1,251.00	1,251.00
63 Servicio de Vigilancia	1,900.00	1,900.00	1,900.00
63 Otros	400.00	500.00	300.00
Alquiler Infraestructura	2,180.00	2,180.00	2,180.00
Material Didáctico	0.00	0.00	0.00
Sub Total Costos	13,256.05	13,316.05	13,106.05
Gastos Administrativos (15%)	1,988.41	1,997.41	1,965.91
Total Egresos UCP Ica	15,244.46	15,313.46	15,071.96
Ingresos UCP Ica	16,000.00	18,000.00	18,000.00
Diferencia	755.54	2,686.54	2,928.04
% Utilidad	4.7%	14.9%	16.3%

Fuente: SENATI Zonal Sur, 2017.

Tabla 12
Pérdidas ocasionadas por posibles desastres

	Enero	Febrero	Marzo
Ingresos CFP ICA general	S/. 16,000.00	S/. 18,000.00	S/. 18,000.00
Ingreso diario	S/. 695.65	S/. 857.14	S/. 947.37
Pérdidas de ingresos por posibles desastres (en base a 1 hora)	S/. 86.96	S/. 107.14	S/. 118.42
Pérdidas de ingresos por posibles desastres (en base a 1 minuto)	S/. 1.45	S/. 1.79	S/. 1.97

Fuente: SENATI Zonal Sur, 2017.

Este trabajo de investigación planteó una solución basándose en la ISO 22301 al tomar en consideración los agentes participantes que se muestran en la Figura 25.

Figura 25
ISO 22301 – Partes Interesadas

Fuente: Norma ISO 22301:2012.

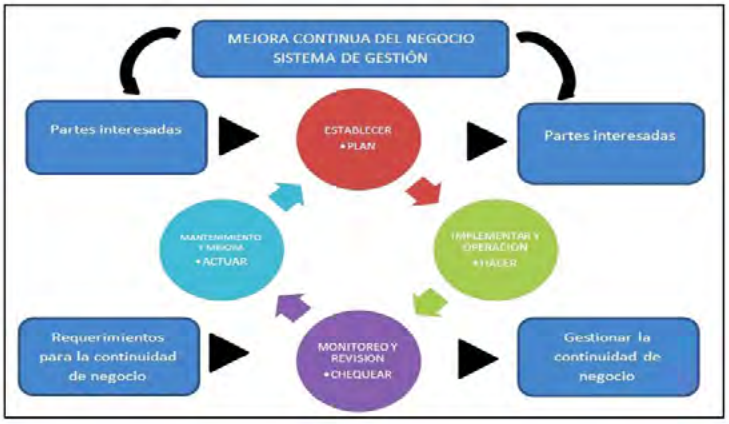
Con el establecimiento de procedimientos y políticas se identificarán las amenazas inherentes al centro de datos, ya sea por desastre natural o inducido, para con ello decretar los riesgos latentes al sistema informático. Es importante recordar el objetivo final, el cual consiste en restablecer la operatividad del servicio en el menor tiempo posible y para ello se

diseñará la arquitectura de red bajo el protocolo IPv6 de tal forma que la réplica y restauración de la data se maneje de forma segura y estable.

Diseñar los controles de seguridad al usar protocolo IPv6 conlleva a un estudio de hardware minucioso ya que la infraestructura actual no atiende los requisitos mínimos para la implementación de este nuevo método de trasmisión; es por ello que se propondrá equipos de red perimetrales, así como también *switch* de *core* permitiendo la viabilidad del proyecto debido a que en la actualidad los proveedores de Internet en Perú como Nextel, Claro, Movistar y Entel ya no cuentan con direcciones IP públicas IPv4 ocasionado por el agotamiento de las direcciones, que son las que por lo común asignan a empresas y/o corporaciones; por consiguiente, la tendencia conlleva desde luego a la utilización de IPv6 y más aún cuando dentro de las políticas de estas compañías proveedoras de Internet tienen como plan a corto plazo migrar toda su red y conectividad a IPv6.

Por otra parte, el Plan de Recuperación de Datos a proponer contempla el nivel de restauración de la data y, por ende, del sistema informático teniendo como base la ISO 22301 "Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos", que aplica el ciclo Plan-Do-Check-Act –PDCA– para la elaboración, establecimiento, aplicación, revisión, mantenimiento y mejora continua de su eficacia y efectividad. A continuación, se muestra el Ciclo del PDCA.

Figura 26
ISO 22301 Estructura



Fuente: Norma ISO 22301: 2012.

Antes de adentrarse a la propuesta de la implementación de un plan de recuperación de datos en caso de desastre en SENATI, ubicado en la región Ica en Perú, es imperativo hablar de los principales riesgos de casos de desastres que pueden ocurrir en la región Ica, debido a que esta región es muy propensa a tener casos de desastres naturales o de otra índole. El Departamento de Ica está ubicado en la costa sur central del litoral peruano y es el único de los departamentos de la costa que está formado por planicies, también llamadas llanuras costeñas. Su altura oscila entre los 2 msnm (Distrito de Paracas - Provincia de Pisco) y los 3.796 msnm (Distrito de San Pedro de Huacarpana - Provincia de Chincha). Los límites del Departamento de Ica son: por el norte con el Departamento de Lima, por el este con los Departamentos de Huancavelica y Ayacucho, por el sur con el Departamento de Arequipa y por el oeste con el Océano Pacífico o Mar de Grau. Además, está situado en la costa central del territorio peruano siendo los puntos extremos de sus coordenadas geográficas los que se detallan en la Tabla 13.

Tabla 13
Límite Región Ica

	Norte	Este	Sur	Oeste
Latitud Sur Longitud Oeste Lugar	12° 57' 42" 75° 36' 43" Punto en el C° Margen límite tripartido entre los departamentos de Ica, Lima y Huancavelica.	13° 53' 18" 76° 23' 48" Punta del Lagarto en el litoral al Sur-Oeste de señal C° Lechuza cota 502.	15° 25' 13" 75° 05' 52" Punta Colorada en el litoral, entre ensenada Chiquerío y ensenada Tres Hermanas.	14° 58 18" 74° 38' 41" Punto en el C° Llano Loma a 3 kms, al NO en línea recta de la margen izquierda de la Quebrada. Carrizal y 5 Kms, SE en línea recta de la margen derecha del río Quemazón.

Fuente: INEI, 2017.

Además, en la Figura 27 se muestra el Mapa Político del Departamento de ICA.

Figura 27
División política Región Ica

Fuente: INEI, 2017.

Además, en la Tabla 14 se muestra las provincias y departamentos de la Región Ica.

Tabla 14
Provincias y Distritos Región Ica

1101 Provincia Ica	1103 Provincia Nazca
1101 Ica	1103 Nazca
1101 La Tinguiña	1103 Chanquillo
1101 Los Aquijes	1103 El Ingenio
1101 Ocucaje	1103 Marcona
1101 Pachacutec	1103 Vista Alegre
1101 Parcona	1104 Provincia Palpa
1101 Pueblo Nuevo	1104 Palpa
1101 Salas	1104 Lupata
1101 San José de Los Molinos	1104 Rio Grande
1101 San Juan Bautista	1104 Santa Cruz
1101 Santiago	1104 Tibillo
1101 Subtanjalla	1105 Provincia Pisco
1101 Tate	1105 Pisco
1101 Yauca Del Rosario	1105 Huancano
1102 Provincia Chincha	1105 Humay
1102 Chincha Alta	1105 Independencia
1102 Alto Laran	1105 Paracas
1102 Chavin	1105 San Andres
1102 Chincha Baja	1105 San Clemente
1102 El Carmen	1105 Tupac Amaru Inca
1102 Grocio Prado	
1102 Pueblo Nuevo	
1102 San Juan De Yanaca	
1102 San Pedro De Huacarpana	
1102 Sunampe	
1102 Tambo De Mora	

Fuente: Gobierno Regional Ica, 2017.

Debido a estos factores y por encontrarse cerca de un río, la región Ica es un departamento que está propenso a que le ocurra desastre de cualquier índole; en las Tablas 15, 16 y 17, se muestran datos antecedentes de los peligros más frecuentes que ha presentado la región Ica.

Tabla 15
Peligros frecuentes Región Ica, año 2008

Fecha	Fenómeno	Departamento	Provincia	Distrito
02/11/2008	Sismo	Ica	Pisco	Pisco
05/09/2008	Sismo	Ica	Ica	Ica
17/07/2008	Marejada	Ica	Chincha	Tambo de Mora
05/06/2008	Inundación	Ica	Ica	Ica
02/04/2008	Precipitaciones	Ica	Ica	Pueblo Nuevo
26/03/2008	Inundación	Ica	Ica	Ocucaje
26/02/2008	Inundación	Ica	Chincha	Tambo de Mora
26/02/2008	Inundación	Ica	Chincha	El Carmen
27/02/2008	Inundación	Ica	Chincha	El Carmen
22/02/2008	Inundación	Ica	Chincha	Alto Laran
15/02/2008	Inundación	Ica	Nazca	Nazca

Fuente: Gobierno Regional Ica, 2009.

Tabla 16
Peligros frecuentes Región Ica, año 2007

Fecha	Fenómeno	Departamento	Provincia	Distrito
22/12/2007	Inundación	Ica	Ica	Ica
15/08/2007	Sismo	Ica	Pisco	Pisco
15/08/2007	Sismo	Ica	Pisco	Paracas
15/08/2007	Sismo	Ica	Chincha	Chincha Alta
15/08/2007	Sismo	Ica	Ica	Ica
03/04/2007	Inundación	Ica	Chincha	El Carmen
02/04/2007	Inundación	Ica	Ica	Los Aquijes
17/02/2007	Inundación	Ica	Ica	Santiago

Fuente: Gobierno Regional Ica, 2009.

Tabla 17
Peligros frecuentes Región Ica, año 2006

Fecha	Fenómeno	Departamento	Provincia	Distrito
09/12/2006	Sismo	Ica	Ica	Ica
26/10/2006	Sismo	Ica	Ica	Ica
20/10/2006	Sismo	Ica	Ica	Ica
16/06/2006	Sismo	Ica	Ica	Ica
31/05/2006	Sismo	Ica	Ica	Ica

Fuente: Gobierno Regional Ica, 2009.

I. Análisis de Riesgos en la Región Ica

En la Tabla 18 se observan los tipos y los indicadores de vulnerabilidad en la región Ica.

Tabla 18
Indicadores de Vulnerabilidad Región Ica

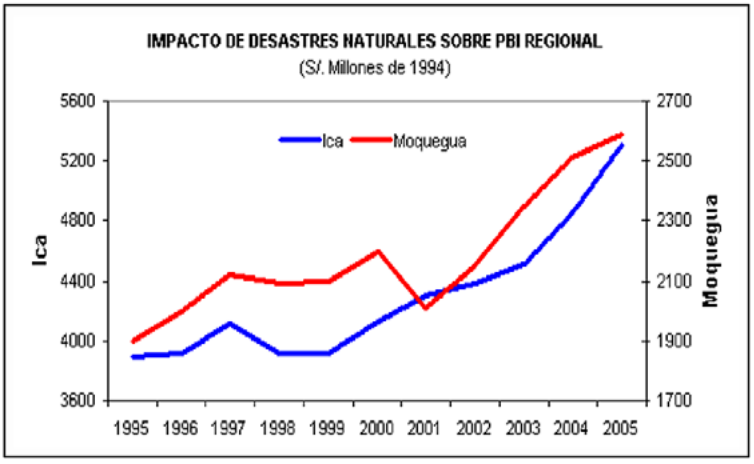
Tipo de Vulnerabilidad	Indicadores de vulnerabilidad identificados en la región	Ámbitos
Física	Ubicación de infraestructura en sectores de alto riesgo	Ubicación de poblaciones, locales institucionales en conos de deyección, franjas marginales o en terrenos eólicos. Carreteras, canales y puentes que atraviesan terrenos inestables
Tecnología	Uso inadecuado de las tecnologías que no responden a las condiciones ambientales existentes y que no permiten el aprovechamiento adecuado de los recursos y oportunidades.	Viviendas de materiales vulnerables a sismos, incendios, vientos, heladas, rayos, etc.
Ambiental	Deforestación de cuencas hidrográficas. Sistemas de producción y actividades extractivas que aceleran el deterioro ambiental. Falta de un desarrollo sostenible para el aprovechamiento de los recursos naturales. Escaso conocimiento en manejo y conservación de suelos Erosión de suelos.	Quebradas secas que se activan con el fenómeno "El Niño" Quebradas y áreas agrícolas no cuentan con defensas vivas Cultivos que demandan mucha agua en época de escasez Actividades mineras y pesqueras artesanales sin el debido asesoramiento.
Social	Debilidades en la organización social: conflictos entre dirigentes y sus bases. Ausencia de organizaciones Deficiente coordinación entre autoridades, líderes y organizaciones de base en el distrito y anexos. Desorganización y desesperación por factores climáticos adversos. Desactivación de comités especiales Desconocimiento de las responsabilidades de los comités Falta de coordinación entre autoridades para el cumplimiento de los acuerdos y la ley. Deficiente presupuesto para la administración, mantenimiento de obras y equipos.	Organizaciones públicas y privadas vulnerables de la Región

Tipo de Vulnerabilidad	Indicadores de vulnerabilidad identificados en la región	Ámbitos
Educativo	Programas curriculares de instituciones educativas que no han insertado las capacidades propuestas por el INDECI y aprobadas por el Ministerio de Educación.	Instituciones Educativas que no desarrollan capacidades de Defensa Civil durante el año lectivo
Institucional	Inestabilidad en las instituciones que traducen en cambios continuos en sus representantes y la carencia de capacidad para tomar decisiones en pro de su desarrollo.	En las instituciones públicas y privadas de la Región
Biológica	Debilidad del sistema fisiológico de salud de las personas y animales que los hacen susceptibles a afectarse ante los cambios climáticos.	Ámbito Regional
Económica	Limitada capacidad económica de las poblaciones para manejar sus riesgos y mejorar las condiciones de seguridad.	Parte de la PEA de la Región

Fuente: INDECI, 2017.

Por otro lado, la economía iqueña representa el 3.6% del PBI Nacional y se concentra, en particular, en: sectores de servicios (58.6%), manufactura (21.3%) y agricultura (13.7%). En el Gráfico 3 se muestra el impacto de los desastres naturales sobre el PBI Regional.

Gráfico 3
PBI Región Ica



Fuente: INEI, 2017.

II. Análisis Cuantitativo de Impacto

En las Tablas 19, 20 y 21 se observa el análisis y la estimación de riesgo de desastre sea el caso.

Tabla 19
Análisis de Sismo

Eje Temático	Elementos expuestos	Vulnerabilidad	Riesgo
Producción	Materia prima Insumo Productos finales (pisco, vino) Infraestructura productiva	Infraestructura insuficiente para pequeños y medianos empresarios. Deficiente innovación tecnológica en pequeñas y medianas empresas Capital de trabajo	Pérdida económica Pérdida de vidas humanas. Escasez e incremento precios.
Vivienda	Infraestructura Servicios básicos (cocina, baños, dormitorio)	Viviendas no resistentes Procesos constructivos deficientes.	Pérdida vidas humanas. Epidemias. Colapso de servicios Traumas
Transporte y comunicación	Carreteras Puentes Sistemas de comunicación	Puentes no resistentes Sistemas de comunicación	Incomunicación Desabastecimiento
Salud	Postas médicas, hospitales, salud física y emocional.	Infraestructura deficiente de equipos materiales. El personal no está capacitado	Pérdidas de vidas humanas y materiales. Enfermedades contagiosas

Fuente: INDECI, 2017.

Tabla 20
Análisis de Tsunami

Eje Temático	Elementos expuestos	Vulnerabilidad	Riesgo
Producción	Planta de gas de camisea Pesca Campos de cultivo, invernaderos. Industrias pesqueras.	Ubicación de plantas pesqueras, gas de camisea y recursos mineros.	Pérdida de capital de inversión. Pérdida de las embarcaciones y vidas humanas. Pérdida de trabajo.
Vivienda	Casas, instituciones públicas y privadas.	Viviendas construidas en zonas no aptas. Limitada capacidad operativa de Defensa Civil. Falta de sensibilidad sobre las amenazas. Autoconstrucción de viviendas.	Colapso e inundación, pérdida de las condiciones de habitad.
Transporte y comunicación	Vías y carreteras afectadas y bloqueadas. Desabastecimiento de productos.	La cercanía al mar Mal estado de las carreteras provoca dificultad en la evacuación.	Transporte interrumpido. Pérdidas de productos perecibles. Colapso de la carretera.
Salud	Daño en la salud de los habitantes de las zonas cercanas y animales.	No se cuenta con los elementos de protección.	Pérdida de vidas.

Fuente: INDECI, 2017.

Tabla 21
Análisis de Inundaciones

Eje Temático	Elementos expuestos	Vulnerabilidad	Riesgo
Producción	Áreas de cultivo Agroindustria Ganado / pecuario	Defensas ribereñas Mala ubicación	Desabastecimiento y escasez producción y agroindustria. Reducción de producción agraria
Vivienda	Población infraestructura habitacional Servicios básicos	Defensas ribereñas Mala ubicación Falta de organización en defensa civil	Viviendas afectadas, colapsadas. Pérdidas.
Transporte y comunicación	Carreteras Fuentes Redes de comunicación	Defensas ribereñas Mal diseño por no considerar el puente hidráulico Estructuras inadecuadas.	Incomunicación Desabastecimiento Recesión de la economía
Salud	Hospitales, centro de salud, postas médicas. Centro de evacuación médica.	Mala ubicación Organización defensa civil inadecuado	Pérdidas de infraestructuras de salud. Riesgos epidemias Equipos

Fuente: INDECI, 2017.

A. Análisis Cualitativo de Impacto

El sector económico de la Región Ica se verá afectado a corto o mediano plazo debido a la destrucción de la infraestructura de los sectores productivos. El efecto del sismo dentro de la Tasa de Crecimiento Nacional, de acuerdo a estimaciones específicas del Poder Ejecutivo, podría alcanzar el 0.3% que, actualizados al valor del PBI nacional, podría representar una pérdida aproximada de 270 millones de dólares hacia finales de año 2017. Sin embargo, este impacto podría aplacarse por el efecto de los comienzos de la construcción en dicha región. Se espera una reactivación de la construcción en Ica debido a los trabajos de reconstrucción en temas de infraestructura, vivienda y servicios básicos por efecto de la inversión pública y privada; proceso que tomará

varios años, pero cuyos efectos iniciales se evidenciarán de inmediato. Por otro lado, se estima un mínimo impacto en la inflación, dado que el abastecimiento de alimentos en la región, que concentra la tercera parte de la población del país, es mínimo.

B. Tipo de Investigación

El presente estudio investigativo reúne las condiciones metodológicas de una investigación no experimental porque se observan situaciones de desastres naturales que ocurren en una entidad técnica privada donde se va a realizar una recolección de datos para diseñar y establecer controles de seguridad al utilizar protocolo IPv6.

C. Descripción del Diseño

El diseño permitió establecer controles de seguridad para recuperación de datos en caso de desastre al usar protocolo IPv6 en una entidad técnica privada, lo que incrementa los niveles de seguridad durante un desastre de la infraestructura actual. Su proceso se puede ver con claridad en el esquema de la Figura 28.

Figura 28
Diseño del proyecto

Fuente: elaboración propia.

En este trabajo investigativo, la población radica en un inventario general de activos de la organización, teniendo la siguiente clasificación:

- Equipos de red: *Routers*, *Switchs* convecionales, *Switch* de core, *Firewall*, IPS.
- Servidores: Base de Datos, Dominio, Archivos.
- Usuarios: Alta Dirección, Gerencias, Jefaturas, TIC, usuarios.
- Proveedor de Servicios de Internet: Movistar, Claro, Nextel
- Organizaciones Afines: Sede Central SENATI, Banco de Crédito del Perú, SUNAT.

Mientras que la muestra son los activos específicos para el modelo de *networking* al usar IPv6 se considera el plan de recuperación de datos: *Router* central, *Firewall* de red local, Servidor de base de datos, Servidor de dominio, Usuarios de Tecnologías de Información.

Por otro lado, dada la naturaleza del tema de estudio y sus objetivos, se seleccionó una investigación descriptiva explicativa porque expresa los principales problemas de la recuperación de datos en caso de desastre lo que deriva en el diseño y establecimiento de controles de seguridad usando el modelo de *networking* IPv6.

Es importante señalar que, para la implementación del proyecto, se necesitaron componentes tanto de hardware como de *software*, además de la mano de obra para el desarrollo. En la Tabla 22 se muestra el estudio de costo de propuestas para el proyecto.

Tabla 22
Costo del proyecto

Proyecto	Período cero	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.	Totales
INGRESOS								
PROGRAMA	S/. 23,225.00	S/. 9,800.00	S/. 10,500.00	S/. 10,500.00	S/. 10,500.00	S/. 10,500.00	S/. 10,500.00	S/. 85,525.00
Documentación	-	S/. 1,000.00	S/. 1,700.00	S/. 1,700.00	S/. 1,700.00	S/. 1,700.00	S/. 1,700.00	S/. 9,500.00
Mantenimiento SW	-	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 5,700.00
Mantenimiento HW	-	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 5,700.00
Materiales								
Papel bond A-4 75 gramos	S/. 72.00	-	-	-	-	-	-	S/. 72.00
Tinta Sistema Continuo Impresora	S/. 50.00	-	-	-	-	-	-	S/. 50.00
Folder manila.	S/. 30.00	-	-	-	-	-	-	S/. 30.00
Lapiceros PILOT BPS-GP (F)	S/. 27.00	-	-	-	-	-	-	S/. 27.00
EQUIPOS								
Laptop HP DV6707 US	S/. 1,800.00	-	-	-	-	-	-	S/. 1,800.00
Impresora Multifuncional F380	S/. 299.00	-	-	-	-	-	-	S/. 299.00
Servidor IBM System x3400 M3 X 2	S/. 6,691.00	-	-	-	-	-	-	S/. 6,691.00
IBM Server 1 TB 7200 SATA 3.5in HS	S/. 5,696.00	-	-	-	-	-	-	S/. 5,696.00
Memoria IBM 2GB (1x2GB) DDR3 1333MHz PC3-10600, ECC,	S/. 2,455.00	-	-	-	-	-	-	S/. 2,455.00
Switch CISCO SF300-48 PUERTOS	S/. 5,000.00	-	-	-	-	-	-	S/. 5,000.00
Mikrotik RB2011L-RM	S/. 405.00	-	-	-	-	-	-	S/. 405.00
SERVICIOS								
Movilidad y viáticos.	S/. 700.00	S/. 5,000.00	S/. 5,000.00	S/. 5,000.00	S/. 5,000.00	S/. 5,000.00	S/. 5,000.00	S/. 15,700.00
EGRESOS								
PERSONAL	-	S/. 18,000.00	S/. 18,000.00	S/. 18,000.00	S/. 18,000.00	S/. 18,000.00	S/. 18,000.00	S/. 108,000.00

Proyecto	Período cero	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.	Totales
INGRESOS								
Coordinador DRP TI		S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 48,000.00
Coordinador de Infraestructura tecnológica		S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 21,000.00
Coordinador de Sistema de Información		S/. 3,000.00	S/. 3,000.00	S/. 3,000.00	S/. 3,000.00	S/. 3,000.00	S/. 3,000.00	S/. 18,000.00
Coordinador de Seguridad de información		S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 21,000.00
Flujo de caja al mes	S/. 23,225.00	S/. 27,800.00	S/. 28,500.00	S/. 28,500.00	S/. 28,500.00	S/. 28,500.00	S/. 28,500.00	S/. 193,525.00

Fuente: elaboración propia.

III. Objetivo general

Desarrollar un Plan de Recuperación de Datos en caso de desastre al diseñar controles de seguridad y al usar protocolo IPv6.

IV. Objetivos específicos

- Evaluar normativas relacionadas con el Plan de Recuperación de Datos en caso de desastres.
- Identificar las amenazas que afectan la operatividad del sistema en caso de desastre.
- Identificar los protocolos de internet en el Plan de Recuperación de Datos contra desastres.
- Determinar el costo económico del diseño de controles de seguridad al usar IPv6 para recuperación de datos en caso de desastre en una entidad técnica privada.

V. Evaluación de normativas relacionadas con el plan de recuperación de datos contra desastres

A través de este plan, se trató desarrollar un sistema que le permita a SENATI-Ica poder manejar e implementar la seguridad de información y la continuidad de negocio en un ambiente de tecnología de información

y plan de negocios. El *diseño y establecimiento de controles de seguridad para Recuperación de Datos en caso de desastre usando protocolo IPv6 en una entidad técnica privada* engloba el desarrollo e implementación de una estructura administrativa y organizativa que presente reportes de los procesos que abarcan todos los aspectos de un plan de continuidad de negocio permitiendo un manejo de negocio efectivo, una continuidad en el servicio brindado y la gestión y administración de los riesgos. De esta manera, el diseño se transforma en una serie de funciones cuyo objetivo es garantizar que la infraestructura de información cuente con un grado de recuperación en caso de que ocurriera un desastre para la continuidad de las actividades que se desarrollan en la organización. Por otro lado, existen secciones que permiten la verificación de que todos los elementos relevantes de seguridad sean desarrollados en una estrategia de continuidad del negocio, las cuales son:

Tabla 23
Evaluación de Normativas

Evaluación de normativas para del desarrollo del diseño		
Normativas	Versión	Sinopsis
iso 22301	2012	La Continuidad de Negocios es un problema latente para todas las organizaciones y su gestión debe ser un elemento esencial de todo el negocio. Ofrece a la organización la capacidad de mantener sus operaciones críticas durante y después de una interrupción, así como de mejorar la velocidad a la que es capaz de establecer su completa funcionalidad.
iso 27001	2013	El Sistema de Gestión de la Seguridad de la Información se basa en la información como conjunto de datos organizados en poder de una entidad que posean valor para la misma. Su seguridad consiste en la preservación de confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.
iso 3100	2009	La Gestión de Riesgo es un conjunto de principios que se deben satisfacer para que sea eficaz cuyo objetivo es integrar el proceso del riesgo en los procesos de la empresa, de estrategia, de planificación y de elaboración de informes como las políticas y los valores.
Ley Protección de Datos Personales n.º 29.733	2011	Tiene el objetivo de garantizar el derecho fundamental a la protección de los datos personales

Fuente: elaboración propia.

VI. Directivas

A. Directiva específica

Desarrollar un Plan de Recuperación de Datos en caso de desastre al usar protocolo IPv6.

Tabla 24
Directiva específica

Directica específica			Código: dire-01 Versión: 01 Aprobado: DN Fecha: 15/12/17 Página:	
Desarrollar un plan de recuperación de datos en caso de desastre al usar protocolo IPv6				
	Cargo	Nombre	Firma	Fecha
Elaborado por:	Analista CN 01 Analista CN 02	César Augusto Cabrera García José Luis Magaño Machacca		
Revisado por:	Asesor 01 Asesor 02	Dra. Carol Cernaqué Miranda Dr. Oswaldo Pelaes León		
Aprobado por:	senati			

Fuente: elaboración propia.

Confidencial: este documento no podrá ser reproducido ni fotocopiado sin la autorización

B. Contenido

Objetivo: establecer los procedimientos necesarios para desarrollar el Plan de Recuperación de Datos en caso de desastre al usar protocolo IPv6.

Alcance: se aplica al sistema sinfo como prueba piloto en la zona Ica.

Desarrollo:

- Políticas de Continuidad de Negocio Alineado iso 22301:2012: la Continuidad de Negocios es un problema latente para todas las organizaciones y su gestión debe ser un elemento esencial de todo el negocio. Su gestión permite a la organización la capacidad de mantener sus operaciones críticas durante y después

de una interrupción, así como de mejorar la velocidad a la que es capaz de establecer su completa funcionalidad.

- Políticas de Sistemas de Gestión de Seguridad de la Información Alineado ISO 27001:2013: se basa en la información como conjunto de datos organizados en poder de una entidad que posean valor para la misma. Su seguridad consiste en la preservación de confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento dentro de una organización.
- Políticas de Gestión de Riesgo Alineado ISO 31000:2009: es un conjunto de principios que se deben satisfacer para que sea eficaz cuyo objetivo es integrar el proceso del riesgo en los procesos de la empresa, de estrategia, de planificación y de elaboración de informes como las políticas y los valores.
- Políticas de Protección de Datos Alineado Ley n.º 29733: esta ley tiene como objetivo el garantizar el derecho fundamental a la protección de los datos personales.

C. Acápites

1. Acápite n.º 01

Políticas de Continuidad de Negocio Alineado ISO 22301:2012.

Tabla 25
Acápite n.º 01

Acápite n.º 01		Código: DIRE-02 Versión: 01 Aprobado: DN Fecha: 15/12/17 Página:		
Políticas de Continuidad de Negocio Alineado ISO 22301:2012				
	Cargo	Nombre	Firma	Fecha
Elaborado por:	Analista CN 01 Analista CN 02	César Augusto Cabrera García José Luis Magaño Machacca		
Revisado por:	Asesor 01 Asesor 02	Dra. Carol Cernaqué Miranda Dr. Oswaldo Pelaes León		
Aprobado por:	SENATI			

Fuente: elaboración propia.

Confidencial: Este documento no podrá ser reproducido ni fotocopiado sin la autorización.

VII. Contenido

Objetivo: evitar interrupciones a los procesos críticos del negocio como consecuencia de fallas o desastres.

Alcance: se aplica al sistema SINFO como prueba piloto en la zona Ica.

A. Políticas generales:

Se consideran los siguientes aspectos:

- Respaldo de información: se establece el esquema de respaldo de la información vital requerida para llevar a cabo cada proceso crítico de negocio.
- Seguridad física: se establecen procedimientos y medidas de seguridad destinadas a salvaguardar los centros de datos, terminales, la estructura física y la información contra eventos naturales o humanos, que de forma intencional o por accidente, puedan afectarlos.
- Mantenimiento del plan: se establecen mecanismos de mantenimiento y actualización del PCN, con el fin de garantizar que se podrá utilizar en efecto ante la materialización de un escenario de crisis, al velar porque su información se encuentre actualizada, completa y precisa.
- Ejercicios del plan: el PCN y Plan de Gestión de crisis son probados con frecuencia, a través de ejercicios realizados por la CCLV, a través de los cuales se evalúa su viabilidad y garantiza que sus empleados estén familiarizados con los planes y procedimientos.

B. Políticas específicas:

Distribución de capacidades de respaldo: los sistemas centrales están replicados en una locación Chiclayo, separado de Ica por una distancia de más de 1.000 km. Mediante las Tablas 26, 27 y 28 se utilizan indicadores para determinar el RPO y RTO.

Tabla 26
Servicio SINFO

Sistema de Información de SENATI –SINFO–			Productos / Servicios
3. Imagen de la compañía	2. Rentabilidad	1. Servicio al cliente	Factores de Impacto Operacional
1. Insignificante	1. Insignificante	1. Insignificante	< 4 hrs
1. Insignificante	3. Moderado	1. Insignificante	< 1 día
1. Insignificante	3. Moderado	2. Menor	< 2 días
2. Menor	4. Mayor	4. Mayor	< 1 sem
3. Moderado	4. Mayor	5. Catastrófico	< 2 sem
5. Catastrófico	5. Catastrófico	5. Catastrófico	< 1 mes
5. Catastrófico	5. Catastrófico	5. Catastrófico	> 1 mes
2 sem			Maximum Tolerable Period of Downtim e (MTPD)
El máximo tiempo de apertura de un curso modular - registro de matrícula es de 2 semanas a partir de esa fecha se hace impostergable el inicio de módulo esto conlleva a no cumplir meta trazadas del mes			Justificación MTPD
1 sem			Recovery Time Objective (RTO)
1 día			Maximum Tolerable Data Loss (MTDL)
El tiempo máximo para considerar una pérdida de datos es de 4 horas a raíz que durante ese periodo resulta insignificante según el análisis realizado caso contrario se perdería data sensible			Justificación MTDL

Fuente: elaboración propia.

Tabla 27
Servicio Apertura de Cursos Modulares

Productos / Servicios		
Factores de Impacto Operacional		
< 4 hrs		
< 1 día		
< 2 días		
< 1 sem		
< 2 sem		
< 1 mes		
> 1 mes		
Maximum Tolerable Period of Downtime (MTPD)		
Justificación MTPD		
Recovery Time Objective (RTO)		
Maximum Tolerable Data Loss (MTDL)		
Justificación MTDL		

APERTURA DE CURSO MODULARES		
3. Imagen de la compañía	2. Rentabilidad	1. Servicio al cliente
1. Insignificante	1. Insignificante	1. Insignificante
1. Insignificante	2. Menor	2. Menor
1. Insignificante	3. Moderado	3. Moderado
2. Menor	3. Moderado	3. Moderado
3. Moderado	4. Mayor	3. Moderado
5. Catastrófico	5. Catastrófico	5. Catastrófico
5. Catastrófico	5. Catastrófico	5. Catastrófico
3 sem		
El máximo tiempo de apertura de un curso modular - registro de matrícula es de 2 semanas a partir de esa fecha se hace impostergable el inicio de módulo esto conlleva a no cumplir meta trazadas del mes		
1 sem		
1 día		
El tiempo máximo para considerar una pérdida de datos es de 4 horas a raíz que durante ese periodo resulta insignificante según el análisis realizado caso contrario se perdería data sensible		

Fuente: elaboración propia.

Tabla 28
Servicio Proceso de Matrícula

Proceso de Matrícula		
3. Imagen de la compañía	2. Rentabilidad	1. Servicio al cliente
1. Insignificante	1. Insignificante	1. Insignificante
1. Insignificante	1. Insignificante	1. Insignificante
1. Insignificante	4. Mayor	2. Menor
2. Menor	4. Mayor	3. Moderado
3. Moderado	4. Mayor	4. Mayor
5. Catastrófico	5. Catastrófico	5. Catastrófico
5. Catastrófico	5. Catastrófico	5. Catastrófico
3 sem		
El máximo tiempo de apertura de un curso modular - registro de matrícula es de 2 semanas a partir de esa fecha se hace impostergable el inicio de módulo esto conlleva a no cumplir meta trazadas del mes		
2 sem		
2 días		
El tiempo máximo para considerar una pérdida de datos es de 1 día a raíz que durante ese periodo resulta insignificante según el análisis realizado caso contrario se perdería data sensible		

Productos / Servicios
Factores de Impacto Operacional
< 4 hrs
< 1 día
< 2 días
< 1 sem
< 2 sem
< 1 mes
> 1 mes
Maximum Tolerable Period of Downtime (MTPD)
Justificación MTPD
Recovery Time Objective (RTO)
Maximum Tolerable Data Loss (MTDL)
Justificación MTDL

Fuente: elaboración propia.

En la Tabla 29 se observa el rol de la localización Chiclayo en estado de normalidad, el Objetivo de Punto de Recuperación –RPO– y el Objetivo de Tiempo de Recuperación –RTO–.

Tabla 29
RPO y RTO SENATI Sede Ica

	CHICLAYO	RPO	RTO
Sistema de Información de SENATI –SINFO–	Activo	1 día	1 semana
Apertura de Programa Modulares	Activo	1 día	1 semana
Proceso de matrícula	Activo	2 días	2 semanas

Fuente: elaboración propia.

Cuando se da el caso donde el rol de varios servicios es activo, se tiene la capacidad para la recuperación automática en caso de ocurrir un desastre. En caso contrario, al momento de ocurrir un desastre, tardaría un tiempo sin servicio durante la ejecución de acciones procesadas hasta restablecer la operatividad.

VIII. Servicios de liquidación y gestión de garantías

El Plan de Recuperación de Datos está concebido para que, en caso de ocurrir cualquier desastre en la sede principal, puedan realizarse las actividades específicas desde una ubicación activa por el tiempo que se precise hasta restaurar la situación de normalidad; incluso puede darse el traslado de personal en caso de ser necesario. Este plan incluye un inventario de recursos técnicos (máquinas, aplicaciones y datos) que se han reaplicado en otro centro de trabajo; además se definen las tareas y el tiempo de ejecución para lograr el correcto funcionamiento del plan. Es imperativo acotar que se hace la revisión del plan cada año y se hacen actualizaciones con la introducción de nuevas modificaciones y servicios.

IX. Infraestructura de Tecnología de la Información

Engloba todos aquellos procedimientos que ameritan la recuperación y el restablecimiento de la normalidad, en caso de ocurrir cualquier desastre, que pueda causar impacto en el hardware, en los servicios de telecomunicación y en las aplicaciones críticas. Además, incorpora el entrenamiento de los técnicos que gestionan todos los recursos informáticos de la infraestructura de información. Tiene como objetivo general el evitar los puntos únicos de fallo tanto en las instalaciones de Miembro como en los nodos de acceso o centros de trabajo.

X. Infraestructura de Sistema Central sinfo

En las sedes principales se han aplicado configuraciones de redundancia automática, en base a duplicación del equipamiento, y configuraciones de alta disponibilidad. El hardware en el que se ejecuta la aplicación sinfo está estructurado por los hosts de la BD y Usuarios, los *arrays* de discos y las unidades de almacenamiento extraíble. En Chiclayo, se presentan dos equipos sincronizados por un mecanismo de réplica local; en su estado normal, la aplicación de sinfo que corre por las máquinas de Ica es el rol activo y los hosts de Chiclayo es el rol pasivo. Del mismo modo, se almacena la información de sinfo en una base de datos en clúster en Ica. Por otro lado, los equipos de Telecomunicación y Seguridad son los *switches*, *routers* y cortafuegos centrales que son sistemas duplicados y dotados de opciones de redundancia automáticas con respaldo adicional en otro centro.

XI. Infraestructura de Nodo de Acceso

Existe un sólo nodo de acceso en la ciudad de Chiclayo y su ubicación coincide con los de los *hosts* centrales.

Líneas de Telecomunicación: los nodos de cada ciudad están interconectados para acceder desde cualquiera de los nodos a cualquiera de los hosts centrales.

Equipos de Telecomunicación: los *routers* emplean mecanismos de redundancia basados en el protocolo hsrp, de manera que cuando

ocurre un fallo en uno de ellos, el otro asume sus funciones manteniéndose la continuidad del servicio. Así mismo, los *switches* están duplicados; para la conexión de los servidores de acceso a los *switches* se considera una distribución de conexiones de manera que el fallo de uno de los *switches* no implique un impacto severo en el servicio al funcionar por lo general los servidores conectados al otro.

XII. Infraestructura de Miembro

Los componentes de una instalación estándar de Miembro se instalan por duplicado de modo que, ante el fallo de cualquier dispositivo o línea, el Miembro puede operar sin necesidad de intervención.

Líneas y equipos de Telecomunicación: se instala una línea de telecomunicación conectadas a nodos; esta línea se conecta a un *router*. El protocolo de *routing* está configurado de modo que queden resueltas de forma automática las situaciones en que se produce un fallo en una de las líneas de telecomunicación. Los *switches* y *routers* tienen las mismas opciones de redundancia que las de los nodos de acceso.

Servidores de acceso: el servidor de comunicaciones Access establece una conexión TCP/IP con los nodos de acceso en donde intercambia mensajes con los sistemas centrales; en este servidor se configura una lista de nodos de acceso con preferencia de conexión asociada a cada uno. La aplicación de este servidor de comunicaciones está dotada de la capacidad de detectar los problemas de conexión a su nodo de acceso principal y, en caso necesario, conmutar siempre al siguiente nodo de acceso de su lista.

XIII. Entorno e Instalaciones Físicas

Los responsables de Seguridad Física mantienen un Plan de Emergencia y de Evacuación, y gestionan los recursos técnicos necesarios para detectar una situación de desastre. Mantienen el control de los procedimientos que deben realizarse al ocurrir un desastre, incluyendo los mecanismos de notificación a las demás personas responsables del plan y los enlaces con las autoridades públicas.

XIV. Plan de formación y pruebas de continuidad

La realización constante de pruebas de continuidad permite la vigencia y eficacia de los planes de recuperación y que todos los integrantes del equipo de recuperación estén familiarizados con los planes. Las consideraciones que se deben tener para la implementación de los procedimientos de continuidad y para la realización de las pruebas de continuidad son:

- El personal que las realice deberá ser como es debido formado antes de su aplicación.
- El personal debe rotar, de manera que todos los integrantes de las diferentes áreas participen en las pruebas.
- La aplicación de pruebas de contingencia no debe poner en riesgo la operación normal de los sistemas.
- Existirá un plan de pruebas de contingencia documentado.
- Las pruebas de contingencia deberán realizarse al menos una vez al año para los elementos que soportan los elementos críticos de negocio.
- Los resultados de las pruebas quedarán de manera apropiada documentados.
- Los componentes individuales se prueban con mayor frecuencia.
- Simulaciones para entrenar en sus respectivos papeles al personal que gestiona las crisis.
- Pruebas de recursos y servicios de proveedores. Ejemplo: Pruebas con líneas de telecomunicación.

XV. Revisión de los planes de continuidad

El Plan de Continuidad se actualiza con la introducción de nuevas tecnologías, los resultados de las simulaciones de desastre, la experiencia de su personal técnico y de dirección, así como mediante la formación constante de los empleados involucrados en el plan. Los planes deben

revisarse como mínimo una vez al año y después de cada auditoría, así como deben revisarse cada vez que se introduzca un cambio significativo en algunos de los Servicios Críticos de Negocio o cuando se identifiquen nuevos riesgos en el Análisis de Impacto de Negocio. Es imperativo acortar que, en este contexto, cualquier revisión en los planes deberá comunicarse por parte del responsable a SENATI.

XVI. Plan de auditorías

En SENATI se auditan cada año tanto aspectos administrativos de los procesos de la Política de Continuidad del Negocio como su estructura, contenido, acciones definidas y la documentación de los procedimientos de control. Estas revisiones son independientes.

XVII. Violaciones a la política

En este caso, si las directivas de SENATI se comprometen a desarrollar este plan, será responsabilidad de ellos no faltar a este compromiso y considerar que la compañía pudiera estar expuesta a procesos legales y contractuales de no realizarlo, poniendo en riesgo el futuro de su operación.

XVIII. Revisión de la política

Esta política puede ser modificada si existiesen cambios en los procesos de negocio de SENATI o en su infraestructura tecnológica; en caso contrario, se debe realizar su revisión cada año.

Acápite n.º 02

Políticas de Sistemas de Gestión de Seguridad de la Información alineado ISO 27001:2013.

Tabla 30
Acápite n.º 02

Acápite n.º 02		Código: DIRE-03 Versión: 01 Aprobado: DN Fecha: 15/12/17 Página:		
Políticas de Sistemas de Gestión de Seguridad de la Información Alineado iso 27001:2013				
	Cargo	Nombre	Firma	Fecha
Elaborado por:	Analista CN 01 Analista CN 02	César Augusto Cabrera García José Luis Magaño Machacca		
Revisado por:	Asesor 01 Asesor 02	Dra. Carol Cernaqué Miranda Dr. Oswaldo Pelaes León		
Aprobado por:	senati			

Fuente: elaboración propia.

Confidencial: este documento no podrá ser reproducido ni fotocopiado sin la autorización

– Contenido

Objetivo: evitar interrupciones a los procesos críticos del negocio como consecuencia de fallas o desastres.

Alcance: se aplica al sistema sinfo como prueba piloto en la zona Ica.

Políticas generales:

- Todo usuario externo que realice operaciones en senati y utilice o tenga acceso a los recursos informáticos, deberá observar lo prescrito en el presente documento. No conocer las políticas no lo exonera de las responsabilidades asociadas con su cumplimiento.
- Los usuarios de senati tendrán acceso a los servicios informáticos y de telecomunicaciones una vez notificado su registro por el área correspondiente de la Gerencia de Operaciones.

- SENATI será responsable de contar con un Plan de Contingencias o recuperación de desastres informáticos para asegurar la continuidad de las operaciones del sistema.
- El Comité de Tecnologías de la Información vigilará que se acaten las políticas de seguridad de la información vigentes a través de la Oficina de Informática.
- Quedará entendido que cualquier acción relacionada con la seguridad de la información que no esté especificada en las presentes políticas está prohibida.
- Políticas y lineamientos específicos:
- SENATI es propietario exclusivo de la infraestructura seguridad SENATI-Ica, de los sistemas de información, talleres y demás que la institución adquiera o desarrolle, en consecuencia, el usuario externo no se beneficiará de ningún derecho de propiedad, en el marco de la utilización de dichos recursos.
- Cualquier forma diferente de ingreso o modificación de información estará sujeta a sanción económica debido al mal uso y probable corrupción de datos que se pudiera generar, de acuerdo con el Reglamento de Infracciones y Sanciones, sin perjuicio de la acción penal correspondiente.
- SENATI contará con servidores como es debido licenciados, para las aplicaciones y Talleres, así como para otras aplicaciones que pudiera desarrollar o adquirir para el funcionamiento del sistema.
- SENATI brindará soporte técnico del servicio de comunicaciones, así como asistencia en línea sobre el manejo de los sistemas y niveles de seguridad apropiados de los sistemas de información de su propiedad; asimismo brindará la capacitación necesaria sobre el uso de los sistemas a los usuarios que así lo soliciten.
- La responsabilidad sobre las claves de acceso a la red, y de los aplicativos otorgados por la Institución serán como corresponde utilizadas y no deberán ser reveladas a personas no autorizadas, para garantizar un adecuado control y funcionamiento de tales aplicativos, deberán considerar que estas contraseñas los identifican.
- Las contraseñas deberán ser cambiadas cada 90 días. Serán mayores a ocho caracteres alfanuméricos y no se podrán repetir las mismas contraseñas utilizadas antes.

- SENATI recomendará el uso de contraseñas al compartir carpetas, el usuario deberá tener la precaución de no compartir las carpetas de los sistemas instalados o configurados por la Institución.

Políticas sobre los bienes informáticos de SENATI:

- Los usuarios externos que utilicen bienes informáticos de SENATI, se responsabilizarán por la pérdida o daño de los mismos. Además, comunicarán al área de Soporte Técnico en caso de fallas de funcionamiento; bajo ninguna circunstancia intentará por sí mismo la reparación de cualquier equipo o componente de éste.
- Toda instalación o mantenimiento de bienes informáticos de *hardware*, de SENATI, reconfiguración de los mismos o de accesorios (tarjetas de red, etc.), será realizada por el Área de Soporte Técnico, quien a su vez llevará el control de dichos mantenimientos.
- SENATI establecerá los lineamientos de seguridad para la protección de los bienes informáticos de su propiedad y apoyará para su efectiva aplicación, así mismo verificará el cumplimiento de los mismos, los usuarios deberán de implementar los lineamientos de seguridad establecidos a fin de salvaguardar la integridad de los equipos asignados por SENATI.

Violaciones a la política: en este caso, si las directivas de SENATI se comprometen a desarrollar este plan, será responsabilidad de ellos no faltar a este compromiso y considerar que la compañía pudiera estar expuesta a procesos legales y contractuales de no realizarlo, poniendo en riesgo el futuro de su operación.

Revisión de la política: esta política puede ser modificada si existiesen cambios en los procesos de negocio de SENATI o en su infraestructura tecnológica; en caso contrario, se debe realizar su revisión cada año**.**

– Acápite n.º 03

Políticas de Gestión de Riesgo alineado ISO 31000:2009

Tabla 31
Acápite n.º 03

Acápite n.º 03		Código: DIRE-04 Versión: 01 Aprobado: DN Fecha: 15/12/17 Página:		
Políticas de Gestión de Riesgo Alineado iso 31000:2009				
	Cargo	Nombre	Firma	Fecha
Elaborado por:	Analista CN 01 Analista CN 02	César Augusto Cabrera García José Luis Magaño Machacca		
Revisado por:	Asesor 01 Asesor 02	Dra. Carol Cernaqué Miranda Dr. Oswaldo Pelaes León		
Aprobado por:	SENATI			

Fuente: elaboración propia.

Confidencial: este documento no podrá ser reproducido ni fotocopiado sin la autorización del SENATI.

– Contenido

Objetivo: evitar interrupciones a los procesos críticos del negocio como consecuencia de fallas o desastres.

Alcance: se aplica al sistema SINFO como prueba piloto en la zona Ica.

– Políticas generales:

Las políticas generales supervisan, controlan y mitigan los riesgos, al mismo tiempo que atenderán a los siguientes principios básicos de riesgo:

- Definir la estrategia y el riesgo e incorporarlas a las decisiones estratégicas y operativas.
- Segregar, a nivel operativo, las funciones entre las áreas de riesgos y las áreas responsables de su análisis, control y supervisión.

- Garantizar la adecuada utilización de los instrumentos para la cobertura de los riesgos y su registro de acuerdo con lo exigido en la normativa aplicable.
- Informar sobre los riesgos y el funcionamiento de los sistemas desarrollados para su control para favorecer la comunicación.
- Alinear con la Política general y gestión de riesgos todas las políticas específicas que sean necesarias desarrollar en materia de riesgos.
- Asegurar el cumplimiento adecuado de las normas establecidas y la actualización y mejora permanente de dicho sistema en el marco de mejorar su seguimiento y medición.

Los principios básicos de la política general de gestión de riesgos se materializan a través de un sistema integral de control y gestión de riesgos apoyado en un Comité de Riesgos y soportado en una adecuada definición y asignación de funciones y responsabilidades a nivel operativo, y en unos procedimientos y herramientas de soporte, adecuados a las distintas etapas y actividades del sistema, que incluye:

- La identificación continua de los riesgos y amenazas relevantes atendiendo a su posible incidencia sobre los objetivos clave de gestión.
- El análisis de riesgos que se realizan con el comité de riesgo.
- El establecimiento de una estructura de políticas, directrices y límites, así como de los correspondientes mecanismos para su aprobación y despliegue, que permitan contribuir de forma eficaz.
- La medición y control de los riesgos siguiendo los procedimientos y estándares.
- El análisis de los riesgos asociados a las nuevas inversiones como elemento esencial en la toma de decisiones en tema de rentabilidad-riesgo.
- El mantenimiento de un sistema de control del cumplimiento de las políticas, directrices y límites, a través de procedimientos y sistemas adecuados, incluyendo los planes de contingencia necesarios para mitigar el impacto de la materialización de los riesgos.

- El seguimiento y control periódico de los riesgos de la cuenta de resultados con el objetivo de controlar la volatilidad del resultado anual del comité de riesgo.
- Los sistemas de información y control interno que permiten realizar una evaluación y comunicación periódica y transparente de los resultados del seguimiento del control y gestión de riesgos, incluyendo el cumplimiento de las políticas y los límites.
- La continua evaluación de la idoneidad y eficiencia de la aplicación del sistema y de las mejores prácticas y recomendaciones en materia de riesgos para su eventual incorporación al modelo.
- La auditoría del sistema por la Dirección de Auditoría Interna.

Políticas y lineamientos específicos:

- La gestión del riesgo crea y protege el valor: Contribuye a la consecución de los objetivos y demostrables de mejora del rendimiento.
- Es una parte integral de todos los procesos de organización: La gestión de riesgos no es una actividad aislada ni separada de las principales actividades y procesos de la organización. Es parte de las responsabilidades de gestión e integrante de todos los procesos de organización, incluida la planificación estratégica, los proyectos y la gestión del cambio.
- La gestión de riesgos es parte de la toma de decisiones: Ayuda a tomar decisiones, priorizar acciones y distinguir entre cursos alternativos de acción.
- Aborda con claridad la incertidumbre.
- La gestión del riesgo es sistemática, estructurada y oportuna: Contribuye a la eficiencia de los resultados consistentes, comparables y fiables.
- Se basa en la mejor información disponible como los datos históricos, la experiencia, la información de los interesados, la observación, los pronósticos y opiniones de expertos. Sin embargo, la decisión de los responsables debe informarse y debe considerar las limitaciones de los datos o modelos utilizados y la posibilidad de divergencia entre los expertos.

- La gestión del riesgo es la medida: Se alinea con el contexto externo e interno de la organización y perfil de riesgo.
- La gestión del riesgo toma en cuenta los factores humanos y culturales: Reconoce las capacidades, las percepciones y las intenciones de las personas internas y externas que pueden facilitar u obstaculizar el logro de los objetivos de la organización.
- La gestión del riesgo debe ser transparente e inclusivo: La adecuada y oportuna participación de los interesados y de los tomadores de decisiones en todos los niveles de la organización asegura que la gestión del riesgo siga siendo pertinente y actualizada. También permite que la participación de las partes interesadas esté con eficacia representada y que sus opiniones sean tomadas en cuenta en la determinación de los criterios de riesgo.
- La gestión de riesgos es dinámica, interactiva y da respuesta al cambio: Como los acontecimientos externos e internos ocurren surgen nuevos riesgos; algunos responden al cambio y otras desaparecen.
- La gestión de riesgos facilita la mejora continua de la organización: Las organizaciones deben desarrollar y aplicar estrategias para mejorar su madurez de gestión de riesgos junto con todos los demás aspectos de la organización.

Violaciones a la política: en este caso, si las directivas de SENATI se comprometen a desarrollar este plan, será responsabilidad de ellos no faltar a este compromiso y considerar que la compañía pudiera estar expuesta a procesos legales y contractuales de no realizarlo, poniendo en riesgo el futuro de su operación.

Revisión de la política: esta política puede ser modificada si existiesen cambios en los procesos de negocio de SENATI o en su infraestructura tecnológica; en caso contrario, se debe realizar su revisión cada año**.**

– Acápite n.º 04

Políticas de Protección de Datos alineado Ley n.º 29733

Tabla 32
Acápite n.º 04

Acápite n.º 04		Código: DIRE-05 Versión: 01 Aprobado: DN Fecha: 15/12/17 Página:		
Políticas de Protección de Datos Alineado Ley n.º 29733				
	Cargo	Nombre	Firma	Fecha
Elaborado por:	Analista CN 01 Analista CN 02	César Augusto Cabrera García José Luis Magaño Machacca		
Revisado por:	Asesor 01 Asesor 02	Dra. Carol Cernaqué Miranda Dr. Oswaldo Pelaes León		
Aprobado por:	senati			

Fuente: elaboración propia.

Confidencial: este documento no podrá ser reproducido ni fotocopiado sin la autorización

– Contenido

Objetivo: impedir las interrupciones a los procesos críticos de la empresa como consecuencia de desastres o fallas.

Alcance: se aplica al sistema sinfo como prueba piloto en la zona Ica.

– Principios generales:

En el desarrollo, análisis e implementación se decretan las disposiciones generales para proteger los datos personales y en las normas que la complementan o modifican se aplicarán los siguientes principios de manera armónica e integral:

- Principio de la legalidad: El tratamiento de datos es una tarea que debe estar sujeta a lo establecido en la ley y a las demás disposiciones que la desarrollen.
- Principio de finalidad: El tratamiento de datos debe acatarse a una finalidad legítima, la cual será informada a la empresa. En cuanto a la recolección de datos personales, senati sólo obtendrá aquellos datos que sean adecuados y pertinentes para el ob-

jetivo por el que fueron requeridos. El director zonal, los jefes zonales, las secretarias, los coordinadores y los instructores se encargarán de informar a la empresa el motivo por el cual se solicita la información y el uso que se le dará a la misma.

- Principio de libertad: el tratamiento solo se puede ejercer con el consentimiento previo del propietario; los datos personales no pueden ser obtenidos o divulgados sin previa autorización.
- Principio de veracidad o calidad: cualquier información que esté sujeta a tratamiento debe ser actualizada, completa, veraz y comprobable; por lo que se prohíbe el tratamiento de datos parciales e incompletos.
- Principio de transparencia: se debe garantizar el derecho del propietario a obtener información del responsable del tratamiento acerca de la existencia de datos que le conciernan en cualquier momento y sin restricciones.
- Principio de acceso y circulación restringida: el tratamiento se sostiene a los límites que se derivan de la naturaleza de los datos personales; por lo tanto, el tratamiento sólo podrá hacerse por personas autorizadas por el propietario y/o por las personas previstas en la ley. De igual forma, los datos personales no pueden estar disponibles en internet o en comunicación masiva, salvo que el acceso sea en teoría controlable para brindar un conocimiento restringido a los titulares o terceros autorizados conforme a la ley.
- Principio de seguridad: la información sujeta a tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros al evitar su adulteración, pérdida, consulta y acceso no autorizado.
- Principio de confidencialidad: SENATI está obligada a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas.

Derechos que le asisten a la empresa que posee la información:

- El conocimiento, actualización y rectificación de los datos personales del propietario frente a SENATI como responsable del tratamiento. Este derecho se podrá ejercer frente a datos parciales e incompletos que induzcan a error o a aquellos cuyo tratamiento esté a propósito prohibido o no haya sido autorizado.
- La solicitud de prueba de la autorización otorgada a SENATI salvo cuando se excluya como requisito para el tratamiento por lo que no es necesaria su autorización.
- Ser informado, por SENATI, sobre el uso que se les ha dado a sus datos personales.
- Deberes de SENATI:
- Garantía constante del pleno y efectivo ejercicio del derecho de hábeas data al propietario.
- Solicitud, conservación y copia de la autorización otorgada por el propietario.
- Información adecuada sobre la finalidad de recolección de datos y los derechos que asisten al propietario en aras de la autorización otorgada.
- Conservación de la información bajo condiciones de seguridad aptas para impedir la consulta, manejo, pérdida o acceso no autorizado.
- Garantía de la información actualizada, comprobable, veraz y completa.
- Actualización de la información en base a las novedades de los datos que atienda el propietario; además, de aplicar las medidas necesarias para la actualización constante de la información.
- Rectificación de la información cuando conveniente o cuando este errónea, al mismo tiempo, se deben comunicar dichos cambios.
- Respeto de las condiciones de seguridad y de la privacidad de la información del propietario.
- Procesar las consultas y los reclamos que son formulados.
- Determinar cuándo alguna información se encuentra en discusión por parte del propietario.
- Avisar al propietario sobre el uso que se les da a sus datos.
- Comunicar a la autoridad de protección de datos cuando se violen los códigos de seguridad y cuando existan riesgos en el manejo de la información de los propietarios.

- SENATI sólo hará uso de los datos personales del propietario para aquellos objetivos que lo necesiten como es debido, al respetar siempre la normativa vigente sobre su protección.

Roles y Responsabilidades:

Se debe asegurar que, dentro de la empresa, la definición de rol y responsabilidad incluya actividades de gestión de seguridad de información; para que sean con claridad definidas es importante que asegurar los siguientes aspectos:

- La línea de reporte debe direccionar a un ejecutivo de alto nivel debido a que, mientras mayor sea su nivel, será más conveniente pues tendrá la influencia necesaria para asegurar que sus administrados implementen el plan de continuidad de negocio.
- Debe existir una coordinación e interacción entre el personal de todas las áreas que pertenezcan a la empresa.
- Identificar los objetivos de protección relacionados con el plan estratégico institucional.
- Identificar los factores clave de seguridad.
- Verificar que los procedimientos y las políticas sean desarrollados y aplicados para asegurar el sustento de la seguridad.
- Identificar todos los controles de seguridad adecuados.
- Adecuada y ordenada implementación de los controles con el personal de las áreas convenientes.
- Implementación de los planes de capacitación de manera que se pueda incluir sesiones para todas las áreas y niveles del negocio.

– Equipo DRP:

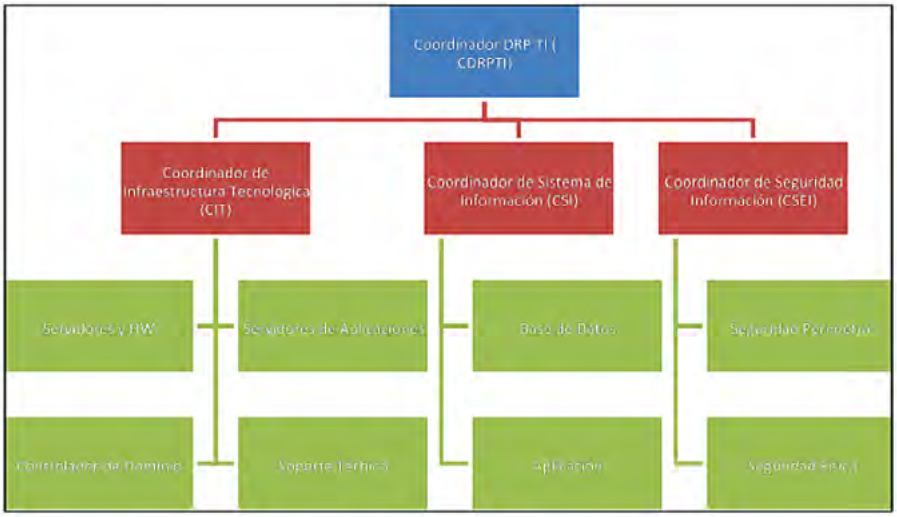
Se hace una identificación de los grupos de personas que están involucradas en el esfuerzo para la recuperación de datos en caso de ocurrir un desastre y las responsabilidades que están asociadas a ellas. Estas son las pautas a considerar para conformar estos grupos:

- Todo grupo debe tener un líder y un alterno.

- No puede haber personas participando en más de un grupo cuyas tareas sean concurrentes durante una recuperación en caso de un desastre.
- Todos sus integrantes deben conocer y reconocer sus responsabilidades para así minimizar las posibilidades de inoperatividad de los equipos a causa de la ausencia de alguno de sus integrantes y a la ignorancia de sus responsabilidades.

Se hace la conformación de los grupos DRP en la Figura 29.

Figura 29
Equipos de DRP TI



Fuente: elaboración propia.

– Responsabilidades del Coordinador DRP TI –CDRPTI–

1. Dirigir, coordinar y decidir acciones y/o estrategias a seguir en un escenario de emergencia sea el caso.
2. Decidir la activación del Plan de Recuperación de Datos en caso de desastres TI.
3. Liderar a los grupos involucrados en el proceso de recuperación.
4. Orientar y supervisar las actividades del personal necesario durante una situación de emergencia.

5. Determinar la gravedad del desastre y las consecuencias que trae sobre la infraestructura tecnológica.
6. Mantener informados a la Alta Dirección acerca de la simulación de desastre, el desarrollo de la recuperación y los posibles problemas que se presentan durante la ejecución de este plan.
7. Documentar las simulaciones de desastres y el empleo de actividades para el logro de la recuperación de las operaciones.
8. Verificar que se ejecuten los procedimientos de recuperación y que se cumpla el cronograma y las prioridades establecidas.
9. Vigilar el proceso de recuperación de infraestructura de TI en el Centro de Datos alterno.
10. Hacer contacto con los proveedores en caso de reemplazar el hardware en los sistemas afectados.
11. Asistir a las reuniones de discusiones sobre el estado de la recuperación y comunicar las necesidades y prioridades que se requieran.
12. Informar la finalización de la ejecución de las operaciones del Plan de Recuperación de Datos en caso de desastres, cuando las operaciones del Centro de Datos primario hayan sido restablecidas.

– Responsabilidades del Coordinador de Infraestructura Tecnológica –CIT–

1. Evaluación del daño en la plataforma tecnológica; dirigir y coordinar todos los procedimientos necesarios para la recuperación en el Centro de Datos alterno y, más tarde, a su restauración.
2. Recuperación de la plataforma de los sistemas críticos en base a la prioridad de recuperación definida.
3. Verificar que toda la documentación relacionada a los procesos de recuperación se ubique en un ambiente seguro.
4. Mantener actualizados los procedimientos de operaciones para poder soportar cualquier aplicación.
5. Mantener la configuración del sistema alterno actualizado y ubicado en un lugar seguro.
6. Vigilar la instalación del software y hardware, así como también mantener configurado versiones recientes de los sistemas operativos en las áreas del Centro de Datos alterno.

7. Recuperación y entrega de las cintas de respaldo del almacenaje externo.
8. Preparación de los procedimientos de backup y restablecimiento de los controles normales de operaciones en el Centro de Datos.
9. Mantenimiento, recuperación y restauración de los enlaces de red y comunicaciones entre la sede principal y el Centro de Datos.
10. Actualización del diagrama actual de conexiones de dispositivos, del diagrama alterno y del inventario de equipos de telecomunicaciones en caso de emergencia.
11. Evaluación del daño en las redes de comunicación de datos y coordinación de las estrategias de recuperación con los proveedores de servicios.

– Responsabilidades del Coordinador de Sistemas de Información – CSI–

1. Levantamiento de los servicios de Base de Datos con la data válida y disponible para los usuarios en el Centro de Datos alterno.
2. Mantener informados a los usuarios sobre los momentos en que se tienen datos confiables.
3. Garantizar el funcionamiento adecuado de las Bases de Datos.
4. Vigilar el funcionamiento adecuado de los diferentes sistemas de aplicación.
5. Verificar la actualización de la documentación de los aplicativos en producción y la contemplación de las actividades de respaldo de los aplicativos en la documentación de operaciones.
6. Elaborar las actividades de recuperación en caso de pérdida de información y/o emergencia.
7. Definir los requerimientos de sistema operativo y la documentación indispensable para el funcionamiento de los aplicativos.
8. Informar a los usuarios sobre los avances de las actividades de recuperación y el restablecimiento de todos los procesos que son sus responsabilidades.
9. Aprobar con el usuario del negocio, el adecuado desempeño de las aplicaciones posterior al restablecimiento de las operaciones en el Centro de Datos alterno.

– Responsabilidades del Coordinador de Seguridad de Información – CSEI–

1. Vigilar que se cumplan los controles que permitan asegurar la integridad, confidencialidad y disponibilidad de la información durante la situación de emergencia.
2. Verificar con los de Seguridad Física, la evaluación del daño en la sede del Centro de Datos.

XIV. Matriz de asignación de responsabilidades –matriz raci–

En la Tabla 33 se muestra la asignación de responsabilidad relacionada con la continuidad de servicio propuesto al utilizar COBIT 4.1 donde I es informado, C es consultado, R es responsable y A es rendir cuentas.

Tabla 33
MATRIZ RACI

DS4 Garantizar la continuidad de servicio											
Marco de Gobierno Cobit 4.1	Ceo Director General	Cfo Jefe De Finanzas	Ejecutivo del Negocio Director de la Sede Ica	Cio CDRPTI	Dueño de Proceso de Negocio CDRPTI	Jefe de Operaciones Sede Ica	Arquitecto en Jefe CIT	Jefe de Desarrollo CSI	Jefe de Administración de TI CSEI	PMO CDRPTI	Cumplimiento, Auditoría, Riesgo y Seguridad CDRPTI
Desarrollar un marco de trabajo de continuidad de TI	I	C	C	A	C	R	R	R	C	C	R
Realizar un análisis de impacto al negocio y valoración de riesgo	I	C	C	C	C	A/R	C	C	C	C	C
Desarrollar y mantener planes de continuidad de TI	I	C	C	C	I	A/R		C	C	C	C

DS4 Garantizar la continuidad de servicio											
Identificar y categorizar los recursos de TI con base en los objetivos de recuperación				C		A/R		C	I	C	I
Definir y ejecutar procedimientos de control de cambios para asegurar que el plan de continuidad sea vigente				I		A/R		R	R	R	I
Probar con frecuencia el plan de continuidad de TI				I	I	A/R		C	C	I	I
Desarrollar un plan de acción a seguir con base en los resultados de las pruebas				C	I	A/R	C	R	R	R	I
Planear y llevar a cabo capacitación sobre los planes de continuidad de TI				I	R	A/R		C	R	I	I
Planear la recuperación y reanudación de los servicios de TI		I	I	C	C	A/R	C	R	R	R	C
Planear e implementar el almacenamiento y la protección de respaldos				I		A/R		C	C	I	I
Establecer los procedimientos para llevar a cabo revisiones post reanudación				C	I	A/R		C	C		C

Fuente: elaboración propia.

XX. Identificación de las amenazas que afectan la operatividad del sistema en caso de desastre y los controles a implementar

– Inventario de Activos

Se elabora un inventario de activos que agrupe los principales activos de información en la empresa. Un activo se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. En la Tabla 34 se muestra los servicios para recuperación de datos en caso de desastre.

Tabla 34
Áreas de Servicio SENATI, sede Ica

ID	SERVICIO	TIPO DE ACTIVO
ZOADICA	Zonal Administrativa Ica	Servicio
DEPTI	Departamento Tecnología de Información	Servicio

Fuente: SENATI, 2017.

Para la medición de los activos usaremos la Tabla 35:

Tabla 35
Valor de los activos

VALORACIÓN DE LOS ACTIVOS	
NIVEL	VALOR
Alto	3
Medio	2
Bajo	1

Fuente: SENATI, 2017.

Tabla 36
Activos según las áreas de servicio SENATI, sede Ica

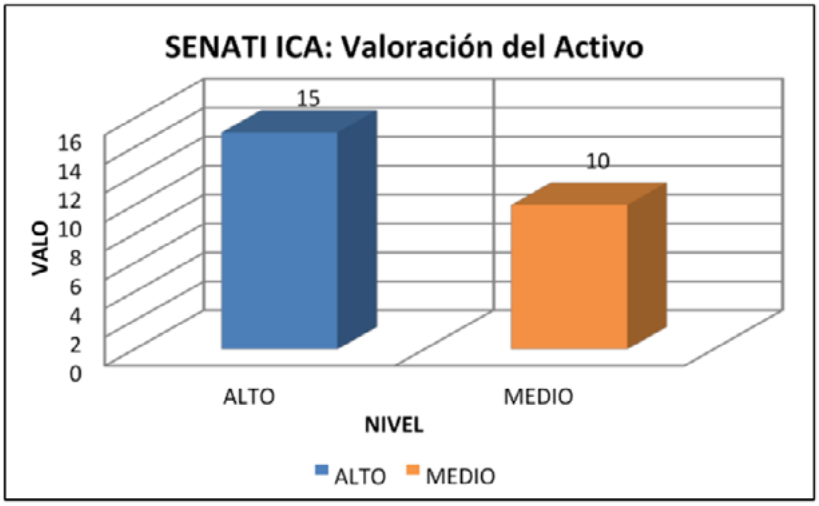
Id	Activo	Cant.	Tipo de Activo	Clasificación Información			Valoración del Activo	
				Conf.	Int.	Disp.	Nivel	Valor
DEPTI	Servidor de Bd - Servidor IBM System X3400 M3	1	Hw	Alto	Alto	Alto	Alto	3
DEPTI	Servidor de usuario - servidor IBM System X3400 M3	1	Hw	Alto	Alto	Alto	Alto	3
DEPTI	Switch CISCO Sf300-48 Puertos	1	Hw	Alto	Alto	Alto	Alto	3
DEPTI	Mikrotik Rb2011l-Rm	1	Hw	Alto	Alto	Alto	Alto	3
DEPTI	Kit de desarmadores ocho piezas	2	Instrumento	-	-	-		
DEPTI	Kit de desarmadores de precisión cinco piezas	2	Instrumento	-	-	-		
DEPTI	Kit de mantenimiento	5	Instrumento	-	-	-		
DEPTI	Kit de soldadura electrónica	5	Instrumento	-	-	-		
DEPTI	Soplador	1	Instrumento	-	-	-		
DEPTI	Multitester analógico	1	Instrumento	-	-	-		
DEPTI	Multitester digital	1	Instrumento	-	-	-		
DEPTI	Testeador de red	2	Instrumento	-	-	-		
DEPTI	Hp Businnes Desktop Pro 4300	1	Hw	Medio	Medio	Medio	Medio	2
DEPTI	Sillas de oficina	2	Inmueble y oficina	-	-	-		
DEPTI	Estantería de oficina	1	Inmueble y oficina	-	-	-		
DEPTI	Escritorio de oficina	1	Inmueble y oficina	-	-	-		
DEPTI	Ventilador de pedestal	1	Inmueble y oficina	-	-	-		
DEPTI	Soporte técnico	1	Persona	Medio	Alto	Medio	Medio	2
DEPTI	Administrador servidor	1	Persona	Alto	Medio	Alto	Alto	3
DEPTI	Sistema Operativo Windows Seven	1	Sw	Medio	Medio	Alto	Medio	2
DEPTI	Sistema operativo Windows Server 208 R2	2	Sw	Alto	Alto	Alto	Alto	3

Id	Activo	Cant.	Tipo de Activo	Clasificación Información			Valoración del Activo	
				Conf.	Int.	Disp.	Nivel	Valor
depti	Infraestructura Depti	1	Infraestructura	Alto	Alto	Medio	Alto	3
zoadica	Sinfo	1	Sw	Alto	Alto	Alto	Alto	3
zoadica	Apertura de programa modular	1	Sw	Alto	Alto	Alto	Alto	3
zoadica	Proceso de matrícula	1	Sw	Alto	Alto	Alto	Alto	3
zoadica	Hp Businnes Desktop Pro 4300	3	Hw	Medio	Medio	Medio	Medio	2
zoadica	Impresora Hp Officejet Pro 8600	1	Hw	Medio	Medio	Medio	Medio	2
zoadica	Sillas de oficina	3	Inmueble y oficina	-	-	-		
zoadica	Sillas metálicas	6	Inmueble y oficina	-	-	-		
zoadica	Estantería de Oficina	1	Inmueble y oficina	-	-	-		
zoadica	Archivador Metálico	1	Inmueble y oficina	-	-	-		
zoadica	Escritorio de Oficina	3	Inmueble y oficina	-	-	-		
zoadica	Ventilador de Pedestal	2	Inmueble y oficina	-	-	-		
zoadica	Jefe Zonal	1	Persona	Alto	Alto	Alto	Alto	3
zoadica	Coordinador General	1	Persona	Alto	Medio	Alto	Alto	3
zoadica	Auxiliar Administrativo	1	Persona	Alto	Medio	Alto	Alto	3
zoadica	Sistema Operativo Windows Seven	3	Sw	Medio	Medio	Alto	Medio	2
zoadica	Infraestructura zoadica	1	Infraestructura	Alto	Alto	Medio	Alto	3

Fuente: senati, 2017.

El Gráfico 4 muestra los inventarios de activos para la recuperación de datos en caso de desastre del sistema sinfo; se muestra la cantidad de activos de alto valor para senati Ica.

Gráfico 4
Valoración del activo SENATI, sede Ica



Fuente: SENATI, 2017.

De los cuales en la Tabla 37, indica los activos de alto valor:

Tabla 37
Activos de Alto Valor SENATI, sede Ica

Id	Activo	Cant.	Tipo de activo	Clasificación información			Valoración del activo	
				Conf.	Int.	Disp.	Nivel	Valor
DEPTI	Servidor de BD - servidor IBM system x3400 m3	1	Hw	Alto	Alto	Alto	Alto	3
DEPTI	Servidor de usuario - servidor IBM system x3400 m3	1	Hw	Alto	Alto	Alto	Alto	3
DEPTI	Switch cisco sf300-48 puertos	1	Hw	Alto	Alto	Alto	Alto	3
DEPTI	Mikrotik rb2011l-rm	1	Hw	Alto	Alto	Alto	Alto	3
DEPTI	Administrador servidor	1	Persona	Alto	Medio	Alto	Alto	3
DEPTI	Sistema operativo windows server 208 r2	2	Sw	Alto	Alto	Alto	Alto	3
DEPTI	Infraestructura DEPTI	1	Infraestructura	Alto	Alto	Medio	Alto	3
ZOADICA	Sinfo	1	Sw	Alto	Alto	Alto	Alto	3

Id	Activo	Cant.	Tipo de activo	Clasificación información			Valoración del activo	
				Conf.	Int.	Disp.	Nivel	Valor
zoadica	Apertura de programa modular	1	Sw	Alto	Alto	Alto	Alto	3
zoadica	Proceso de matrícula	1	Sw	Alto	Alto	Alto	Alto	3
zoadica	Jefe zonal	1	Persona	Alto	Alto	Alto	Alto	3
zoadica	Coordinador general	1	Persona	Alto	Medio	Alto	Alto	3
zoadica	Auxiliar administrativo	1	Persona	Alto	Medio	Alto	Alto	3
zoadica	Infraestructura zoadica	1	Infraestructura	Alto	Alto	Medio	Alto	3

Fuente: senati, 2017.

Estos activos de alto valor son parte del Sistema Información sinfo senati donde su infraestructura se encuentra alojada en: Infraestructura Departamento de Tecnología - Información –depti– e Infraestructura Zonal Administrativo Ica –zoadica–.

XXI. Amenazas

– *Desastre natural*

Los fenómenos naturales son aquellos ocasionados por el constante movimiento y transformación de la naturaleza, como pueden ser los terremotos, sismos, lluvias, erupciones volcánicas, huracanes, tornados, entre otros; y pueden provocar grandes pérdidas humanas y materiales, en parte por la falta de planificación de medidas preventivas y de seguridad. De la misma manera, estos fenómenos naturales se convierten en desastre cuando superan un límite de normalidad, por lo general, medido por un parámetro; y que varía de acuerdo al tipo de fenómeno.

XXII. Tipos de desastres naturales en Ica

– Inundación

Causado por la acumulación de lluvias y agua en un lugar concreto; se produce por lluvias continuas, o una fusión rápida de grandes cantida-

des de hielo, o ríos que reciben un exceso de precipitación y se desbordan. En la Tabla 38 se muestra el grado de desastre por lluvias fuertes e inundaciones en Ica durante el periodo 2003-2011.

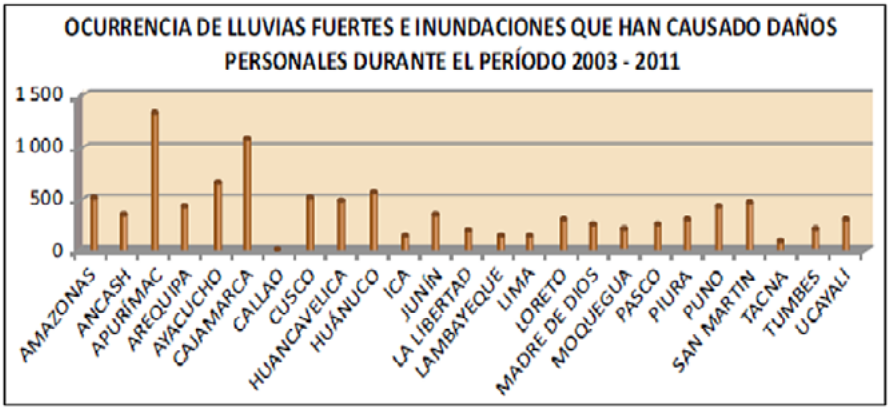
Tabla 38
Desastre por lluvias fuertes e inundaciones en la Región Ica

DEPARTAMENTO	EMERGENCIAS	POBLACION DAMNIFICADA	POBLACION AFECTADA
	LLUVIAS E INUNDACIONES	LLUVIAS E INUNDACIONES	LLUVIAS E INUNDACIONES
TOTAL NACIONAL	9 126	315 442	2 636 151
AMAZONAS	537	4 839	28 427
ANCASH	323	1 301	19 829
APURÍMAC	1 378	6 540	324 757
AREQUIPA	411	2 734	160 032
AYACUCHO	654	19 860	119 124
CAJAMARCA	1 055	10 723	159 420
CALLAO	8	24	150
CUSCO	537	26 159	97 827
HUANCAVELICA	513	5 303	86 424
HUÁNUCO	563	10 013	236 739
ICA	50	1 646	34 471
JUNÍN	323	16 187	22 840
LA LIBERTAD	148	6 081	21 240
LAMBAYEQUE	109	8 571	80 195
LIMA	76	480	1 655
LORETO	253	95 319	496 922
MADRE DE DIOS	202	6 651	30 462
MOQUEGUA	160	10 923	57 066
PASCO	197	1 536	5 347
PIURA	296	23 820	179 485
PUNO	401	30 545	96 831
SAN MARTÍN	471	10 701	144 486
TACNA	34	397	17 523
TUMBES	186	627	127 406
UCAYALI	241	14 462	87 493

Fuente: INDECI, 2013.

En el Gráfico 5 se muestra la ocurrencia de lluvias en Perú en donde ocurren con frecuencia en Apurímac y en Cajamarca.

Gráfico 5
Ocurrencia de Inundaciones en la Región Ica



Fuente: INDECI, 2013.

– Sismo

Fenómenos que son impredecibles, se da en las placas tectónicas de la corteza terrestre y pueden provocar desastres como los tsunamis o erupciones volcánicas. En la superficie, se manifiesta por un movimiento o sacudida del suelo, y puede dañar enormemente las estructuras mal construidas. En la Tabla 39 se muestra el grado de desastre por sismos en Ica durante el periodo 2003-2011.

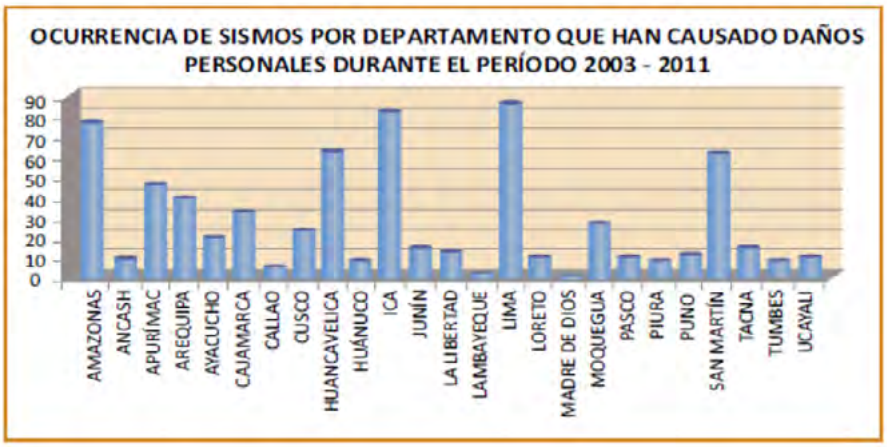
Tabla 39
Desastre por sismos en la región Ica

DEPARTAMENTO	EMERGENCIAS	POBLACIÓN DAMNIFICADA	POBLACIÓN AFECTADA
	SISMOS	SISMOS	SISMOS
TOTAL NACIONAL	645	440 602	286 472
AMAZONAS	74	3 738	7 768
ANCASH	10	0	13
APURÍMAC	45	190	35 235
AREQUIPA	40	200	193
AYACUCHO	21	1 395	4 066
CAJAMARCA	32	1 682	1 049
CALLAO	3	0	0
CUSCO	22	1 156	4 629
HUANCAVELICA	61	11 420	20 996
HUÁNUCO	6	6	226
ICA	82	352 614	157 406
JUNÍN	13	727	1 935
LA LIBERTAD	11	98	1 154
LAMBAYEQUE	1	0	0
LIMA	85	55 020	36 214
LORETO	7	60	405
MADRE DE DIOS	0	0	0
MOQUEGUA	28	3 006	2 939
PASCO	6	291	178
PIURA	4	0	0
PUNO	8	30	80
SAN MARTÍN	60	8 917	11 846
TACNA	15	52	140
TUMBES	5	0	0
UCAYALI	6	0	0

Fuente: INDECI, 2013.

En el Gráfico 6 se muestra la ocurrencia de sismos en Perú en donde ocurren con frecuencia en Amazonas, Huancavelica, Ica, Lima y San Martin.

Gráfico 6
Ocurrencia de sismos en la Región Ica



Fuente: INDECI, 2013.

XXIII. Tipos de Sismos

Subducción: Puede producir los terremotos de mayor magnitud. La placa oceánica se desplaza por debajo de la corteza continental y hacia el magma del manto, donde es consumida y reciclada.

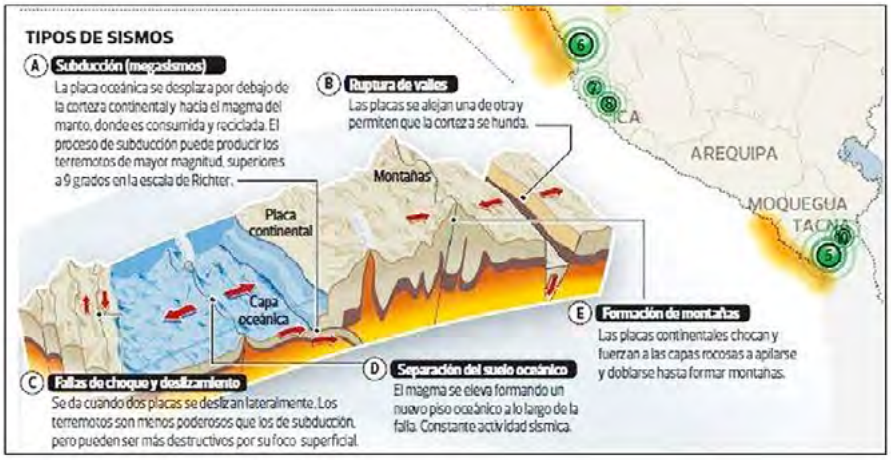
*Ruptura de valles***:** Las placas se alejan una de otra y permiten que la corteza se hunda.

Fallas de choque y deslizamiento: Se da cuando dos placas se deslizan de forma lateral. Los terremotos son menos poderosos que los de subducción, pero puede ser más destructivo por su foco superficial.

Separación del suelo oceánico: El magma se eleva al formar un nuevo piso oceánico a lo largo de la falla. Constante actividad sísmica.

En la Figura 30 se muestra los tipos de sismos mediante la placa tectónica.

Figura 30
Tipo de sismos



Fuente: Diario El Comercio, 2017.

– Tsunami

Ola gigante de agua que alcanza la orilla con una altura superior a 15 metros; pueden ser causados por terremotos. En la Tabla 40 se muestra el grado de desastre por tsunamis en Ica durante el periodo 1996-2007.

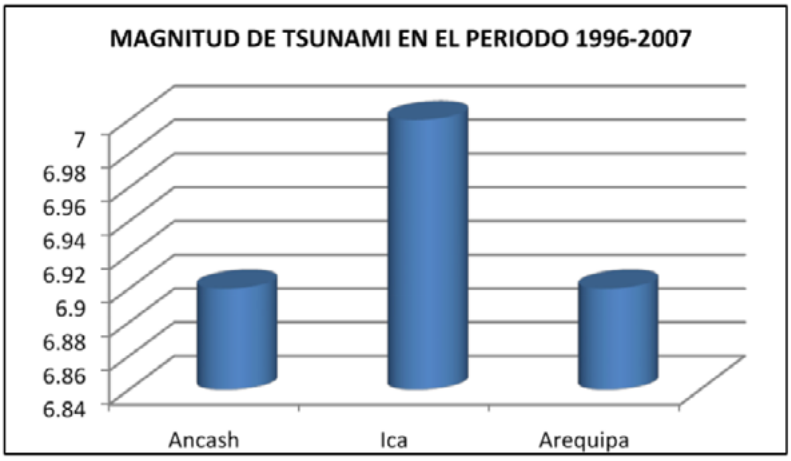
Tabla 40
Magnitud de Desastre

Departamento	Magnitud en Escala de Richter
Ancash	6.9°
Ica	7.0°
Arequipa	6.9°

Fuente: Dirección de Hidrografía y Navegación.

En el Gráfico 7 se muestra la magnitud de tsunami en Perú donde Ica posee una magnitud de 7.0° en Escala de Richter.

Gráfico 7
Magnitud de Tsunami en la Región Ica



Fuente: INDECI, 2010.

XXIV. Tipos de desastres antrópicos en Ica

– Incendios

Fuego no controlado que puede abrasar algo que no está destinado a quemarse y puede afectar a estructuras y a seres vivos. En la Tabla 41 se muestra los desastres antrópicos en la región Ica.

Tabla 41
Desastres Antrópicos en la región Ica

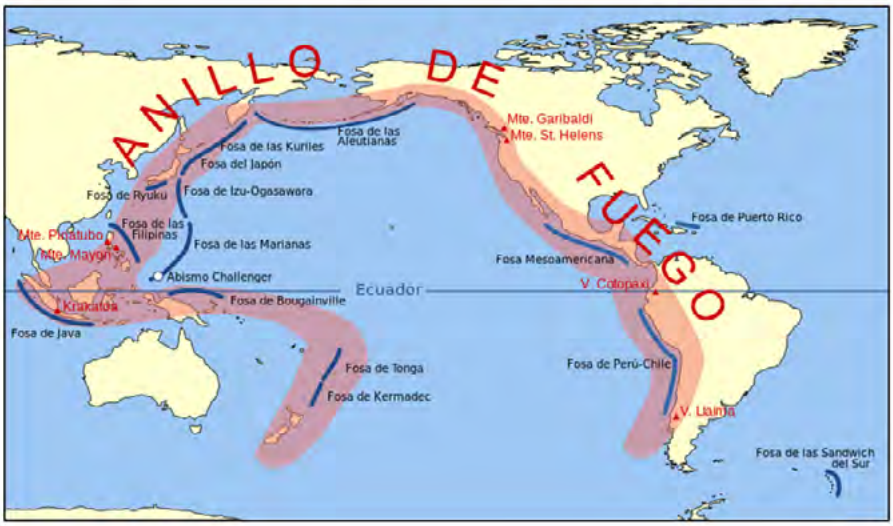
Año 2008				
Fecha	Fenómeno	Departamento	Provincia	Distrito
07/09/2008	Incendio urbano	Ica	Nazca	Nazca
10/08/2008	Incendio urbano	Ica	Ica	Ica
24/07/2008	Incendio urbano	Ica	Nazca	Nazca
06/04/2008	Incendio urbano	Ica	Ica	Ica
07/02/2008	Incendio urbano	Ica	Ica	Ica
Año 2007				
09/05/2007	Incendio urbano	Ica	Ica	San Juan Bautista
10/04/2007	Incendio urbano	Ica	Pisco	Tupac A, Inca
23/03/2007	Incendio urbano	Ica	Nazca	Marcona
22/02/2007	Incendio urbano	Ica	Ica	Ica
Año 2006				
31/10/2006	Incendio urbano	Ica	Ica	Ica
21/06/2006	Incendio urbano	Ica	Pisco	Pisco
03/06/2006	Incendio urbano	Ica	Pisco	Pisco
15/03/2006	Incendio urbano	Ica	Nazca	Nazca
19/02/2006	Incendio urbano	Ica	Ica	Ica
08/01/2006	Incendio urbano	Ica	Pisco	Pisco
02/01/2006	Incendio urbano	Ica	Ica	Ica

Fuente: Gobierno Regional Ica, 2010.

– Cinturón de Fuego del Pacífico

Está situado en las costas del océano Pacífico y se caracteriza por concentrar algunas de las zonas de subducción más importantes del mundo, lo que ocasiona una intensa actividad sísmica y volcánica en las zonas que abarca. En la Figura 31 se visualiza el anillo de fuego.

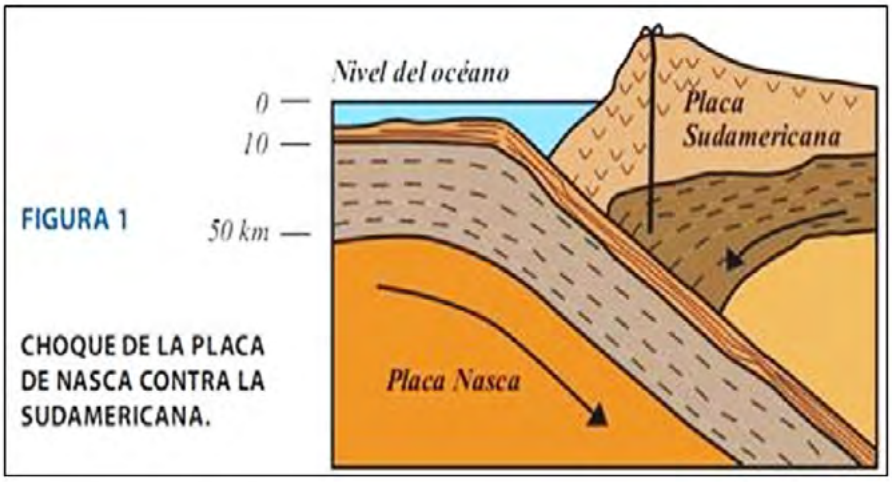
Figura 31
Cinturón de Fuego



Fuente: INDECI, 2010.

El lecho del océano Pacífico reposa sobre varias placas tectónicas, las cuales están en permanente fricción y, por ende, acumulan tensión que, cuando se libera, origina terremotos en los países del cinturón. Además, las placas de la corteza terrestre se hunden a gran velocidad (varios centímetros por año) y a la vez acumulan enormes tensiones que deben liberarse en forma de sismos. En la Figura 32 se muestra la placa de Nazca donde se refleja la fricción entre la placa Sudamericana.

Figura 32
Placa de Nazca



Fuente: INDECI, 2010.

– Placas Tectónicas

Pueden llegar a ser reconocidos como elementos geográficos que toman una mayor importancia siendo las culpables de la gran cantidad de sismos y terremotos que puede llegar a sentirse en el mundo. Entre las placas oceánicas se pueden destacar a la Placa de Nazca, ubicada en el océano Pacífico oriental, ante todo en la costa occidental de Sudamérica, frente las naciones de Chile, Perú, Ecuador y parte de Colombia. En la Figura 33 se muestra la estructura de la Placa de Nazca y la corteza continental.

Figura 33
Estructura de la Placa de Nazca

Fuente: INDECI, 2010.

– Compendio Desastres Naturales en Ica

Teniendo antecedentes históricos sobre desastres naturales en la región Ica, se elabora detalle estadístico sobre los desastres comunes en Ica para evaluar la amenaza existente en la región.

– Estadísticas Sísmicas en la Región Ica

El Instituto Geofísico del Perú –IGP– es una institución pública al servicio del país que forma parte del Ministerio del Ambiente y que contribuye a la gestión del ambiente geofísico con énfasis en la prevención y mitigación de desastres naturales y antrópicos. En la Figura 34 se visualiza la intensidad de sismos en la región Ica al considerar este desastre como una amenaza latente.

Figura 34
Intensidad de sismos en la Región Ica

Fuente: Instituto Geofísico del Perú, 2013.

En la Figura 35 se segmenta la región Ica para visualizar la profundidad del sismo.

Figura 35
Segmentación de Sismos por la Región Ica

Fuente: Instituto Geofísico del Perú, 2013

En la Tabla 42 se muestra la magnitud de los desastres en la región Ica haciendo un cruce de información con Instituto Geofísico del Perú (Sismos), Dirección de Hidrografía y Navegación del Perú (Tsumani), Senamhi (Inundaciones) y Oficina Departamental Estadística e Informática ICA-INEI.

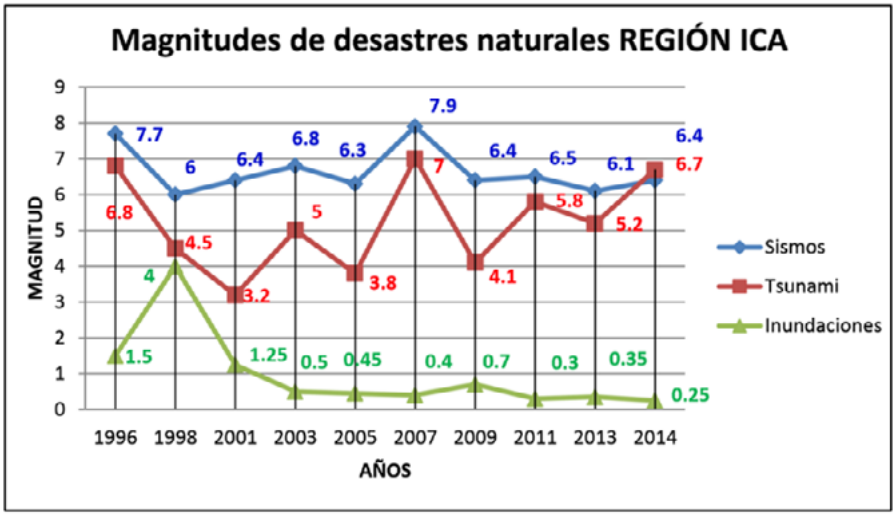
Tabla 42
Muestra Estadística de Desastres en la Región Ica

	1996	1998	2001	2003	2005	2007	2009	2011	2013	2014
Sismos	7.7°	6°	6.4°	6.8°	6.3°	7.9°	6.4°	6.5°	6.1°	6.4°
Tsunami	6.8°	4.5°	3.2°	5°	3.8°	7.0°	4.1°	5.8°	5.2°	6.7°
Inundaciones	150 m^3/s	400 m^3/s	125 m^3/s	50 m^3/s	45 m^3/s	40 m^3/s	70 m^3/s	30 m^3/s	35 m^3/s	25 m^3/s

Fuente: elaboración propia.

En el Gráfico 8 se observa la tendencia frecuente de desastre natural como el sismo y el tsunami en la región Ica.

Gráfico 8
Magnitud de Desastres naturales en la Región Ica



Fuente: elaboración propia.

– Cuadro de Amenaza

Una vez obtenido la identificación de la amenaza de los desastres naturales de la Región Ica se procederá a la amenaza según activos y el nivel de amenaza, según se observa en la Tabla 43.

Tabla 43
Cuadro de amenaza

Área	Activo	Amenazas de desastre			Valoración Del Desastre	
		Sismos	Tsunami	Inundaciones	Nivel	Valor
depti zoadica	Servidor de Bd - Servidor ibm System X3400 M3	Alto	Alto	Medio	Alto	3
	Servidor de usuario - Servidor Ibm System X3400 M3	Alto	Alto	Medio	Alto	3
	Switch cisco Sf300-48 Puertos	Alto	Alto	Medio	Alto	3
	Mikrotik Rb2011l-Rm	Alto	Alto	Medio	Alto	3
	Sinfo	Alto	Alto	Medio	Alto	3
	Apertura de Programa Modular	Alto	Alto	Medio	Alto	3
	Proceso de Matrícula	Alto	Alto	Medio	Alto	3
	Infraestructura zoadica	Alto	Alto	Medio	Alto	3

Fuente: elaboración propia.

En la Tabla 44 muestra que las amenazas con mayor frecuencia son:

Tabla 44
Nivel de Amenaza

	Nivel de amenaza
Sismos	Alto
Tsunami	Alto
Inundaciones	Medio

Fuente: elaboración propia

XXV. Análisis de Impacto al Negocio –BIA–

– Cuestionario

En la Tabla 45 se especifica los servicios ofrecidos en SENATI:

Tabla 45
Servicios ofrecidos por SENATI

	Descripción del Producto / Servicio / Proceso		Frecuencia & Picos de la operación		
#	Producto / Servicio	Descripción del Producto / Servicio	Frecuencia (unid / mes)	Tiempo pico en el día (de HH:MM a HH:MM)	Tiempo pico en el mes
1	**SINFO (SISTEMA DE INFORMACIÓN DE SENATI)**	SISTEMA DE INFORMACIÓN DONDE SE ALOJA LOS MÓDULO DE: - NRC (CURSOS) - DOCENTES - ALUMNOS. - NOTAS	300 OPERACIONES AL MES	8:00 A 16:00	PRIMERA SEMANA DEL MES
2	**APERTURA DE CURSO MODULARES**	EL REGISTRO DE INGRESOS DE ALUMNOS EN EL NRC CREADO: - HORARIO - FRECUENCIA - DURACIÓN	4 OPERACIONES AL MES	14:00 A 16:00	PRIMERA SEMANA DEL MES
3	**PROCESO DE MATRÍCULA**	REGISTRO DE MATRÍCULA MEDIANTE EL NRC CREADO POR SINFO	120 OPERACIONES AL MES	14:00 A 16:00	PRIMERA SEMANA DEL MES

Fuente: elaboración propia.

En la Tabla 46 se especifican las entradas y salidas de información de los servicios ofrecidos en SENATI:

Tabla 46
Entradas y salidas de información

#	Servicios	Entrada de información	**Área proveedora de información**	Tipo de registro	Salida de información	**Área receptora de información**
1	Sistema de Información de SENATI – SINFO–	Módulo de matricula	Coordinación académica	Registro en el sistema de información	Reporte de id de alumnos	Director Departamental y registro Académicos
		Módulo de notas	Coordinación académica	Registro en el sistema de información	Récord Académico	Director Departamental y Registros Académicos
		Módulo cursos	Coordinación académica	Registro en el sistema de información	Reporte de NRC	Director Departamental y Registro Académicos
2	Apertura de Cursos Modulares	Nombre del curso, duración, costo, participantes	Jefatura zonal	Registro en el sistema de información	Malla curricular	Director Departamental y Registro Académicos
		Datos de docente, experiencia, pago de honorarios	Coordinación académica	Registro en el sistema de información	Reporte a Cursos a dictar	Director Departamental y Registro Académicos
3	Proceso de matrícula	Datos del alumno	Coordinación académica	Registro en el sistema de información	Reporte Cumplimiento de Metas	Director Departamental y Registro Académicos
		Curso a Matricularse	Coordinación académica	Registro en el sistema de información	Reporte Cumplimiento de Metas	Director Departamental y Registro Académicos

Fuente: elaboración propia

En la Tabla 47 se especifican los registros vitales para la ejecución de servicios ofrecidos en SENATI:

Tabla 47
Registros vitales de SENATI, Sede Ica

#	Servicios	Nombre del Registro	Clasificación de la Información	Descripción del Registro	Tipo de registro	Frecuencia de Respaldos	Recovery Point Objective –RPO–
1	Sistema de Información de SENATI – SINFO –	Credenciales de autenticación	Uso Interno	En el VPN se da acceso mediante CUSU (Área de Soporte) para generar las cuentas de usuarios antes validadas	Email	mensual	semanal
		Manual de usuario	Uso Interno	Guía de ayuda para interactuar con el sistemas de información	Email	anual	mensual
2	Apertura de curso modulares	Malla de cursos por zonal	Uso Interno	Cursos ingresado en el año lectivo	Sistema de información	anual	mensual
		File del docente	Confidencial	Currículo vitae	Email	semestral	mensual
3	Proceso de matrícula	Ficha de matrícula	Uso Interno	Fichas ingresadas en el año lectivo	Sistema de información	mensual	mensual
		Registro de actas	Uso Interno	Nóminas de inicio y término de curso	Sistema de información	mensual	mensual

Fuente: elaboración propia.

– Riesgo

Acápite n.º 05
Identificación de Peligros, Evaluación de Riesgos –IPER–

Tabla 48
Acápite n.º 05

Acápite n.º 05		Código: DIRE-03 Versión: 01 Aprobado: DN Fecha: 15/12/17 Página:		
Identificación de Peligros, Evaluación de Riesgos –iper–				
	Cargo	Nombre	Firma	Fecha
Elaborado por:	Analista CN 01 Analista CN 02	César Augusto Cabrera García José Luis Magaño Machacca		
Revisado por:	Asesor 01 Asesor 02	Dra. Carol Cernaqué Miranda Dr. Oswaldo Pelaes León		
Aprobado por:	senati			

Fuente: elaboración propia.

Confidencial: este documento no podrá ser reproducido ni fotocopiado sin la autorización

– Contenido

Objetivo: establecer una metodología para identificar peligros en los procesos definidos por la Institución. Evaluar sus riesgos asociados, determinar los riesgos significativos.

Alcance: abarca a todas las actividades ligadas a la formación y capacitación profesional, servicios técnicos y otras actividades de la institución, que se realicen tanto dentro como fuera de sus instalaciones.

Definiciones:

- Peligro: acto o situación con potencial de daño.
- Riesgo: probabilidad de ocurrencia de una exposición o evento peligroso.
- Evento Peligroso: suceso de cualquier índole descrito en base a su severidad, ubicación y sus características.
- Consecuencia: aquello que sigue, de manera asociada y conjunta, provocado por un acto o un hecho.

- Riesgo Significativo: aquel riesgo que se ubica en un nivel de consecuencia de tal manera que no puede ser aceptado por la Institución.
- Riesgo Aceptable: aquel riesgo ubicado en un nivel que puede ser tolerado por la empresa, al tener en cuenta su propia política y sus obligaciones legales.
- Probabilidad: escala de medida que define la posibilidad de ocurrencia de un suceso.
- Severidad: intensidad de las consecuencias ocurridas durante un suceso.
- Categorización: estructura de elementos en una determinada categoría.
- IPER: identificación de peligros, evaluación de riesgos.

Responsabilidades:

Directores Zonales y Jefes de CFP/UFP/Responsables de Área/ Escuelas.

- Proporcionar los recursos necesarios para la aplicación del presente procedimiento.
- Comunicar al personal bajo su responsabilidad el resultado de la IPER.

Miembros de los Comités de Gestión Zonal o CFP

- Identificar peligros, evaluar riesgos, determinar los riesgos significativos y realizar la reevaluación de los riesgos significativos al aplicar la metodología desarrollada en este acápite.
- Comunicar a todo el personal el resultado de la IPER y asegurar su entendimiento y aplicación.

Prevencionista de Riesgos

- Capacitar al personal en la aplicación del presente acápite.
- Participar en la IPER y en la determinación de los controles al asegurar su eficacia.
- Participar y asegurar la actualización de las matrices de IPER.

- Verificar el cumplimiento de los controles operacionales definidos en las matrices de IPER.

Personal de la institución (Administrativos e instructores)

- Participar en la IPER de la organización
- Reportar nuevos peligros identificados en el lugar de trabajo
- En el caso de instructores, informar a los alumnos sobre la IPER.

Desarrollo: revisión de los procesos y determinación de actividades: teniendo definido el proceso a evaluar, los miembros del Comité de Gestión Zonal o CFP, Directores Zonales, Jefes de CFP/ Responsables de Área/ Escuelas, apoyados por el personal involucrado, determinan el conjunto de actividades que conforman dicho proceso. Esta etapa es el punto de partida para la identificación de peligros y riesgos asociados a cada actividad.

Identificación de peligros y riesgos asociados:

- Identificar la zonal/CFP/UFP/Área o Escuela donde se realizan las actividades.
- Detallar las actividades que conforman el proceso y verificar si son rutinarias, no rutinarias o de emergencia.
- Anotar la familia ocupacional, ambiente, frecuencia con la que se realiza la actividad (diario, semanal, mensual o semestral), número de personas involucradas, y fecha actualizada del registro.
- Distinguir los peligros y los riesgos asociados a la actividad realizada al interior o exterior de las instalaciones de la empresa.

Determinación de la Significancia de Riesgos y Propuesta de Controles:

Aquellos riesgos identificados suelen ser evaluados por el Comité Zonal de Gestión o CFP, Directores Zonales, Jefes de CFP/UFP/Escuela y/o Responsables de Área, con el fin de determinar, de acuerdo a su severidad y probabilidad de ocurrencia, cuáles son riesgos significativos, para así plantear medidas de seguridad que permitan minimizar dichos riesgos de acuerdo a estas etapas:

a) Determinación del Valor de la Probabilidad (P): este valor se calcula de acuerdo a los siguientes índices: Índice de personas expuestas (IPE), Índice de procedimientos existentes (IPr), Índice de capacitación (IC) e Índice de frecuencia (IF). Cada índice se caracteriza por tener valores predeterminados por la Institución, seleccionados en base a la naturaleza del riesgo. En la Tabla 49 se encuentran detallados estos valores.

Tabla 49
Evaluación de la Probabilidad

Índice	Probabilidad (P = IPE + IPr + IC + IF)			
	Personas expuestas (IPE)	Procedimientos (IPr)	Capacitación (IC)	Frecuencia (IF)
1	De 1 a 15	Existen/ son satisfactorios	Personal capacitado	Semestral (al menos una vez al semestre)
2	De 16 a 30	Existen en parte/ No son satisfactorios	Personal en parte capacitado	Mensual (al menos una vez al mes)
3	Más de 31	No existen	Personal no capacitado	Diario (al menos una vez al día)

Fuente: elaboración propia.

El valor de la probabilidad del riesgo es la suma de los valores de cada índice:

$$\mathbf{P = IPE + IPr + IC + IF}$$

b) Determinación del Índice de Severidad (S): este valor se calcula en función a la magnitud del daño. En la Tabla 50 se presentan los parámetros establecidos para determinar su valor.

Tabla 50
Evaluación de la Severidad

Índice	Severidad
1	Leve
2	Dañino/ reversible
3	Muy dañino/irreversible

Fuente: elaboración propia.

c) Determinación del Grado de Riesgo (GR): este grado es el producto de la multiplicación de los valores de la probabilidad y severidad. Se determina si el riesgo es significativo o no, en función a los parámetros establecidos por la Institución y a su valor obtenido (ver Tabla 51).

Grado de riesgo = Probabilidad x Severidad

Tabla 51
Determinación de la significancia del riesgo y control propuesto

Grado del riesgo			
Grado de riesgo	Significancia		Control Propuesto
Hasta 16	Aceptable	No significativo	No requiere controles adicionales
Hasta 24	Moderado	Significativo	Requiere programar e implementar controles
Hasta 36	Inaceptable	Significativo	Requiere análisis y programar e implementar controles de inmediato

Fuente: elaboración propia.

En este caso, se identifican los Riesgos Significativos como aquellos que, por su grado de riesgo, se caracterizan por ser inaceptable y moderado, y que requieran una acción a tomar. Por otro lado, los Riesgos No Significativos son aquellos cuyos grados de riesgo se ubican hasta el rango 16 por lo que no requieren ningún control adicional a los que ya se realizan y los esfuerzos se centrarán en mantener los controles para los riesgos que resultaron ser significativos.

XXVI. Actualización de Peligros/Riesgos

Las matrices de IPER deben actualizarse como mínimo una vez al año, cuando aparezca un nuevo requisito legal o cuando cambien las condiciones de operación en las actividades o servicios que brinda el SENATI y se originen nuevos peligros/riesgos; de esto se encargará el prevencionista de riesgos. Así mismo, se debe realizar la determinación de peligros, evaluación de riesgos.

Tabla 52
Infraestructura ZOADICA (Zonal Administrativa Ica) cuadro IPER

N.º	Peligro	Riesgo		Evaluación								Control propuesto
				Índice	IPE	IPr	IC	IF	P = IPE+IPr+	S	GR=PxS	
		Evento	Consecuencia	1	1 a 15	Existen	Capacitado	Semestral		Leve	Hasta 16	Aceptable	No Requiere Control
				2	16 a 30	Parcial	Parcial	Mensual		Dañino/ Reversible	Hasta 24	Moderado	Requiere control
				3	> 31	No existen	No Capacitado	Diario		Muy Dañino/ irreversible	Hasta 36	Inaceptable	Análisis y Control inmediato
1	Partes del equipo en movimiento	Atrapamiento	Contusiones, cortes, laceraciones		3	1	1	2	7	2	14	Aceptable	
2	Ruido	Exposición	Molestias auditivas		3	1	1	2	7	1	7	Aceptable	
			Estrés, fatiga		3	1	1	2	7	1	7	Aceptable	
3	Proyección de partículas	Contacto, incrustación	Laceraciones, afectación a los ojos		3	1	1	2	7	2	14	Aceptable	
4	Energía Eléctrica	Contacto, electrocución	Quemaduras		3	1	1	2	7	2	14	Aceptable	
5	Superficies punzocortantes	Contacto	Cortes, punzones		3	1	1	2	7	2	14	Aceptable	
6	Polvo metálico	Inhalación	Afecciones respiratorias		3	2	2	2	9	2	18	Moderado	
7	Posturas prolongadas	Exposición	Dolores musculares		3	1	1	2	7	2	14	Aceptable	
8	Sismo	Movimiento terrestre	Contusiones, cortes, laceraciones, Destrucción Activos		3	3	3	2	11	3	33	Inaceptable	PROPUESTA PROYECTO TESIS
9	Tsumani	Aumento de olas	Contusiones, cortes, laceraciones, Destrucción Activos		3	3	3	2	11	3	33	Inaceptable	PROPUESTA PROYECTO TESIS
10	Inundaciones	Aumento de caudal	Contusiones, cortes, laceraciones, Destrucción Activos		3	3	3	2	11	3	33	Inaceptable	PROPUESTA PROYECTO TESIS
11	Incendios	Exposición	Contusiones, cortes, laceraciones, Destrucción Activos		3	1	1	2	7	2	14	Aceptable	

Fuente: elaboración propia.

Tabla 53

Infraestructura DEPTI (Departamento Tecnología de Información cuadro IPER

N.º	Peligro		Riesgo		Evaluación								Control propuesto
				Índice	IPE	IPr	IC	IF	P = IPE+IPr+	S	GR=PxS		
		Evento	Consecuencia	1	1 a 15	Existen	Capacitado.	Semestral		Leve	Hasta 16	Aceptable	No Requiere Control
				2	16 a 30	Parcial	Parcial	Mensual		Dañino/ Reversible	Hasta 24	Moderado	Requiere control
				3	> 31	No existen	No Capacitado	Diario		Muy Dañino/ irreversible	Hasta 36	Inaceptable	Análisis y Control inmediato
1	Partes del equipo en movimiento	Atrapamiento	Contusiones, cortes, laceraciones		3	1	1	2	7	2	14	Aceptable	
2	Ruido	Exposición	Molestias auditivas		3	1	1	2	7	1	7	Aceptable	
			Estrés, fatiga		3	1	1	2	7	1	7	Aceptable	
3	Proyección de partículas	Contacto, incrustación	Laceraciones, afectación a los ojos		3	1	1	2	7	2	14	Aceptable	
4	Energía Eléctrica	Contacto, electrocución	Quemaduras		3	1	1	2	7	2	14	Aceptable	
5	Superficies punzocortantes	Contacto	Cortes, punzones		3	1	1	2	7	2	14	Aceptable	
6	Polvo metálico	Inhalación	Afecciones respiratorias		3	2	2	2	9	2	18	Moderado	
7	Posturas prolongadas	Exposición	Dolores musculares		3	1	1	2	7	2	14	Aceptable	
8	Sismo	Movimiento terrestre	Contusiones, cortes, laceraciones, Destrucción Activos, Desastre Natural		3	3	3	2	11	3	33	Inaceptable	PROPUESTA PROYECTO TESIS
9	Tsumani	Aumento de olas	Contusiones, cortes, laceraciones, Destrucción Activos, Desastre Natural		3	3	3	2	11	3	33	Inaceptable	PROPUESTA PROYECTO TESIS
10	Inundaciones	Aumento de caudal	Contusiones, cortes, laceraciones, Destrucción Activos, Desastre Natural		3	3	3	2	11	3	33	Inaceptable	PROPUESTA PROYECTO TESIS
11	Incendios	Exposición	Contusiones, cortes, laceraciones, Desastre Antrópico Destrucción Activos		3	2	2	2	9	2	18	Moderado	

Fuente: Elaboración propia.

Tabla 54
Controles de Seguridad IPv6 cuadro IPER

Control de seguridad en IPv6	ISO 22301:2012	ISO 27001:2013	ISO 31000:2009	Ley Peruana n.º 29733 – Protección de Datos Personales
Monitorear la trazabilidad de la red a nivel de paquetes entrantes y salientes Adquirir y poner a prueba las herramientas de monitoreo y evaluación de IPv6	Seguimiento y monitoreo de los datos y resultados (clausula n.º 9.1.1)	Registro de eventos que afecten la seguridad de la información en la red corporativa (a.12.4.1) las redes se deben proteger y monitorear para asegurar la información en los sistemas y aplicaciones (a.13.1.1)	Monitorear y revisar a menudo los Procesos para garantizar Que los controles son eficaces e identificar riesgos emergentes (cláusula n.º 5.6)	La organización debe asegurar el tratamiento de los datos personales con medidas técnicas, organizativas y Legales (título I - artículo 9)
Desactivar IPv6 en toda la Organización para asegurar que no existan rutas desconocidas en la red. Incluye interfaces y protocolos de túnel	La organización determina el campo de aplicación. Define el ámbito e identifica los servicios y actividades Críticas (cláusula n.º 4.3.2)	Las áreas de responsabilidad cuentan con restricciones y políticas que reducen la posibilidad de concurrencia de información, deben establecerse canales y reglas definidas que resguarden la seguridad de la Información (a.6.1.2)	El contexto interno de cada una de las áreas alinea la gestión de riesgos con los procesos y su estructura en un marco de alcanzar los objetivos de la organización (cláusula n.º 5.3.3)	El principio de legalidad trata la recopilación de datos conforme a lo establecido en la ley, en consecuencia los mecanismos de conectividad deben ser explícitos y lícitos (título I - artículo 4)

Control de seguridad en IPv6	iso 22301:2012	iso 27001:2013	iso 31000:2009	Ley Peruana n.º 29733 – Protección de Datos Personales
Planificar en base a los requerimientos para construir la seguridad que la organización necesita al utilizar ipv6 en la capa de aplicación	La planificación considera los requerimientos declarados en base al contexto de la organización. Determina los riesgos y oportunidades que necesitan ser dirigidos (cláusula n.º 6.1)	La organización establece requisitos para la seguridad de la información y la continuidad de la gestión. Contempla situaciones adversas y medidas de contingencia (a.17.1.1)	Tratar el riesgo implica planificar implementación de controles en procesos cíclicos de valoración, Mitigación y estandarización (cláusula n.º 5.1.1)	El tratamiento de los datos personales no debe extenderse a otra finalidad, en efecto, la planificación de actividades debe estar reguladas mediante Procedimientos y políticas de Seguridad (título i - artículo 6)
Hacer un piloto IPv6 en un sector de la red al utilizar una tecnología de transición. Desarrollar un plan de transición para toda la red en IPv6 de forma incremental	Las evaluaciones deben ser realizadas con frecuencia Con el objetivo de analizar y reportar los cambios significativos que deben plasmarse en procedimientos oportunos (cláusula n.º 9.1.2)	Las pruebas de funcionalidad deben llevarse a cabo durante el desarrollo y despliegue (a.14.2.8) las actualizaciones, nuevas versiones y adaptaciones deben establecer programas de aceptación y criterios de Implantación (a.14.2.9)	La finalidad de evaluar el riesgo es facilitar la toma de decisiones, en base a los resultados se prioriza la implementación del tratamiento (cláusula n.º 5.4.4)	Los datos personales deben ser Exactos, veraces y actuales en la medida que sea posible. El tratamiento de la información debe garantizar su seguridad (título i – artículo 8)
Ejecutar planes de control sin parar debido a que el número de vulnerabilidades en la red de su organización Aumentará en masa	Mejora continua (clausula n.º 10.2)	Los sistemas deben revisarse con frecuencia para determinar el cumplimiento con las políticas Y normas de seguridad (a.18.2.3)	Los indicadores de gestión del riesgo deben establecer las metas de desempeño de la organización (anexo a.3.1)	El valor de los principios debe regirse basado en criterios de Mejora continua (título i - artículo 12)

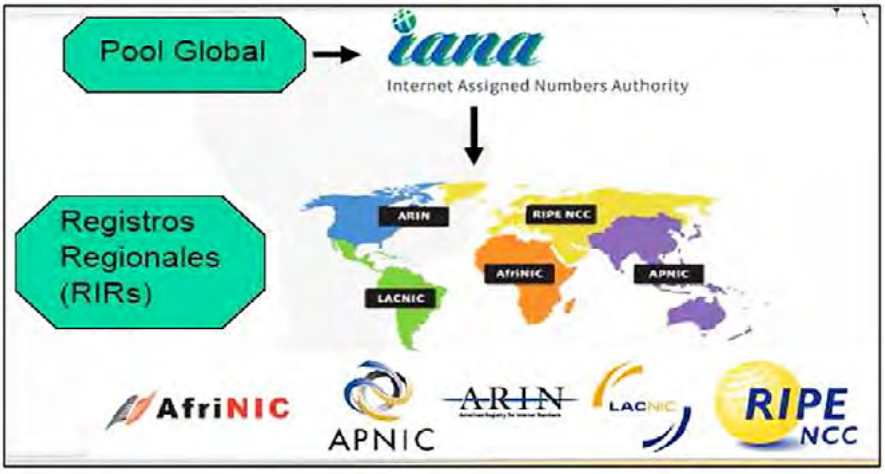
Fuente: elaboración propia.

XXVII. Identificación de los protocolos de internet en el Plan de Recuperación de Datos contra desastre

Modelo de *Networking* para el Sistema de Recuperación de Datos en caso de desastre

El interés de plantear una propuesta de modelo de *Networking* en IPv6 se origina, en especial, por el decaimiento de las direcciones IPv4 y por la mala distribución en cada uno de sus tipos de redes (A, B, C). Por ejemplo, una dirección tipo A permite millones de *host*, pero una organización no cuenta con este dimensionamiento por lo que desperdicia una gran cantidad de direcciones tipo A, así como se añaden problemas de seguridad, criptográficos. Por consiguiente, la tendencia hacia IPv6 es natural debido a que la IETF plantea una nueva versión de IP que es capaz de producir estándares "abiertos". Una de las primeras soluciones a la problemática del IPv4 fue conocida como Simple IP Plus –SIPP–, en donde se realizaba un aumento del tamaño de las direcciones IP a 64 *bits* al mejorar ciertos aspectos de IPv4. Esta solución era lo que necesitaría Internet después de ciertas modificaciones. Sin embargo, las direcciones logran pasar de 64 bits a 128 bits y es cuando se le asigna el nombre de IPv6. En la Figura 36 se muestra la distribución de direcciones según la IANA.

Figura 36
Distribución de direcciones IANA



Fuente: IANA, 2006.

Es imperativo acortar que los Protocolos de Internet Versión 4 y Versión 6 estarán en funcionamiento y coexistirán por un largo tiempo. Sin embargo, es importante elaborar mecanismos de introducción para el IPv6, debido a que esto permitirá la conexión a las redes. Algunos de ellos pueden ser: dual Stack, túneles, 6to4, 6over4. En la Tabla 55 se pueden resumir las características principales del IPv6.

Tabla 55
Características principales del IPv6

Direccionamiento	128 *bits*
Enrutamiento	Direccionamiento jerárquico
Presentación	Cabecera simple de 40 Byte, alineada de a 64 *bits*, y cualquier otra información se agrega como cabecera en extensión (opcional)
Versatilidad	Formato flexible de opciones
Multimedia	Id de flujos
Multicast	Obligatorio
Seguridad	Soporte de autenticación y cifrado
Autoconfiguración	Tres métodos PnP
Movilidad	Source routing, seguridad, detección de móviles, hand-off
Fragmentación	Tan solo de extremo a extremo, es decir que sólo el origen puede fragmentar. Para implementar esto, hace uso de PMTU (Path MTU, RFC 1191), que es el mecanismo empleado para determinar la máxima unidad de datos que contendrá un datagrama, una vez conocido este tamaño, armará todos los paquetes sin superar el mismo, por ende ningún router deberá fragmentarlo pues no será necesario
Tamaño de datagrama	Mantiene el mismo concepto que la versión 4 y propone un nuevo modelo de datagrama, llamado Jumbograma, el cual se define a través de una cabecera en extensión, y permite transmitir datagramas de hasta 4 Gbyte. La idea de esta nueva aplicación es permitir la transmisión de grandes volúmenes de datos entre servidores, los cuales no necesitan incrementar con tanta redundancia de cabecera, siendo el mejor representante de esto el empleo de clúster de servidores

Fuente: CISCO, 2008.

Para enfrentar la problemática de la implementación de IPv6 sobre IPv4, en la Tabla 56 se hará un enfoque en los siguientes pasos:

Tabla 56
Implementación de IPv6 sobre IPv4

Tarea	Descripción	Instrucciones
1. Preparar el *hardware* que admitirá IPv6	Comprobar que el *hardware* pueda actualizarse a IPv6	Se detectan las entidades de la red que sean compatibles con IPv6. La mayoría de las veces, la implementación de IPv6 no modifica la topología de red (cables, routeadores y hosts). Antes de configurar direcciones IPv6 en interfaces de red, debe preparar para IPv6 el hardware y las aplicaciones y verificar que el hardware de la red se pueda actualizar a IPv6. Por ejemplo, consulte la documentación de los fabricantes sobre la compatibilidad con IPv6 respecto a los siguientes tipos de *hardware*: *Routeadores*, *Firewall*, Servidores y Conmutadores
2. Disponer de un ISP que admita IPv6	Comprobar que el ISP admita IPv6. Se pueden utilizar dos ISP, uno para IPv6 y otro para comunicaciones de IPv4	Un proveedor de servicios de Internet –ISP– es una empresa dedicada a conectar a Internet a los usuarios, o las distintas redes que tengan, y a dar el mantenimiento necesario para que el acceso funcione de forma correcta; también ofrece servicios como alojamiento web o registro de dominios, etc.
3. Comprobar que las aplicaciones estén preparadas para funcionar con IPv6	Verificar que las aplicaciones puedan funcionar en un entorno IPv6	Actualice los servicios de red para que admitan IPv6, como los servidores de correo, servidores NIS y NFS. Verificar que el hardware del servidor de seguridad ya esté preparado para IPv6. Verificar que otros servicios de red se hayan conectado a IPv6. Si el sitio implementa los servicios siguientes, asegurar las medidas apropiadas: Servidores de seguridad. - Para poder admitir IPv6, quizá deba incrementar la severidad de las directrices ya establecidas para IPv4. Correo. - En los registros MX para DNS, quizá deba agregar la dirección IPv6 del servidor de correo. DNS. - Para cuestiones específicas de DNS. IPQoS
4. Disponer de prefijo de sitio.	Solicite al ISP o al RIR más próximo un prefijo de sitio de 48 bits.	Debe obtenerse una dirección fija de IP antes de configurar IPv6.

Tarea	Descripción	Instrucciones
5. Crear un plan de direcciones de subredes.	Planificar la topología de red IPv6 global y el esquema de direcciones para poder configurar IPv6 en los distintos nodos de la red.	Traducción de direcciones IPv4 a IPv6 Prefijo de subred (Equivalencias) IPv4 IPv6 192.168.1.0/24 2001:db8:3c4d:1: :/64192.168.2.0/24 2001:db8:3c4d:2: :/64192.168.3.0/24 2001:db8:3c4d:3: :/64192.168.4.0/24 2001:db8:3c4d:4::/64
6. Diseñar un plan para el uso de túneles.	Establezca los routeadores que deben ejecutar túneles a otras subredes o redes externas.	La implementación de IPv6 permite varias configuraciones de túneles para actuar como mecanismos de transición cuando la red migra a una combinación de IPv4 e IPv6. Los túneles posibilitan la comunicación entre redes IPv6 aisladas. Como en Internet se ejecuta en su mayoría IPv4, los paquetes de IPv6 del sitio deben desplazarse por Internet a través de túneles hacia las redes IPv6 de destino.
7. Crear un plan de direcciones para entidades de la red.	Se debe planificar la dirección de servidores, routeadores y hosts antes de configurar IPv6.	Creación de un plan de direcciones IPV6 para nodos. En la mayoría de los hosts, la configuración automática sin estado de direcciones IPv6 para sus interfaces constituye una estrategia válida y eficaz. Cuando el host recibe el prefijo de sitio del ruteador más próximo, el protocolo ND genera de forma automática direcciones IPv6 para cada interfaz del host.
8. Desarrollar directrices de seguridad de IPv6.	A la hora de desarrollar directrices de seguridad de IPv6, consulte las funciones de filtro IP, arquitectura de seguridad IP (IPsec), Internet Key Exchange (IKE) y otras funciones de seguridad de Solaris.	Esta sección se centra en la seguridad de red. La arquitectura de seguridad IP (IPsec) protege la red en el nivel del paquete. El intercambio de claves de Internet (IKE) administra las claves para IPsec. El filtro IP de Solaris proporciona un cortafuego.

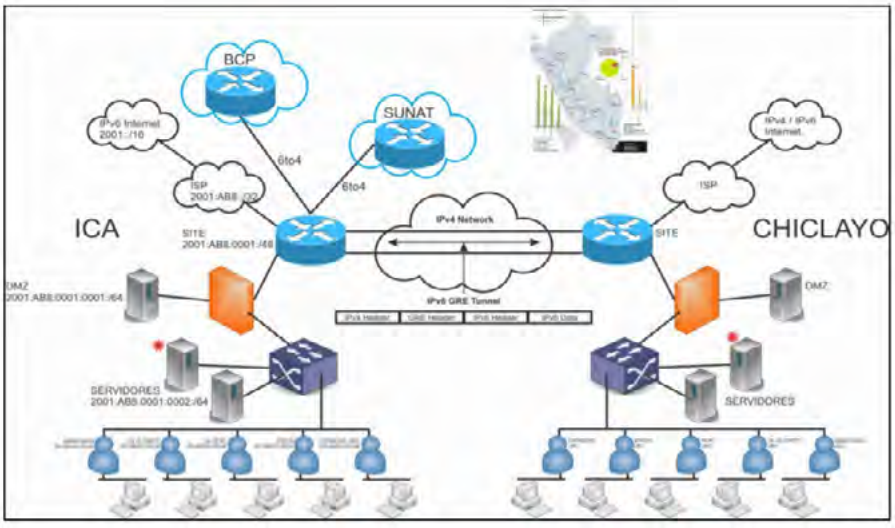
Tarea	Descripción	Instrucciones
9. (Opcional) Configurar una DMZ.	Por motivos de seguridad, se precisa un plan de direcciones para la DMZ y sus entidades antes de configurar IPv6.	Al implementar IPv6 en una red ya configurada, debe tener la precaución de no poner en riesgo la seguridad del sitio. Durante las sucesivas fases en la implementación de IPv6, tenga en cuenta los siguientes aspectos relacionados con la seguridad: Los paquetes de IPv6 e IPv4 necesitan la misma cantidad de filtrado. A menudo, los paquetes de IPv6 pasan por un túnel a través de un servidor de seguridad. Los nodos de IPv6 son a nivel mundial asequibles desde fuera de la red empresarial. Si la directiva de seguridad prohíbe el acceso público, debe establecer reglas más estrictas con relación al servidor de seguridad. Por ejemplo, podría configurar un servidor de seguridad con estado.

Fuente: elaboración propia.

XXVIII. Diseño Topológico

En la Figura 37 se muestra el diseño topológico SENATI.

Figura 37
Diseño Topológico de Red



Fuente: elaboración propia.

Detalle de las instrucciones:

XXIX. Topología de Red

Mediante la Tabla 57 se muestra paquete de IPv6.

Tabla 57
Cabecera fija de un paquete de IPv6

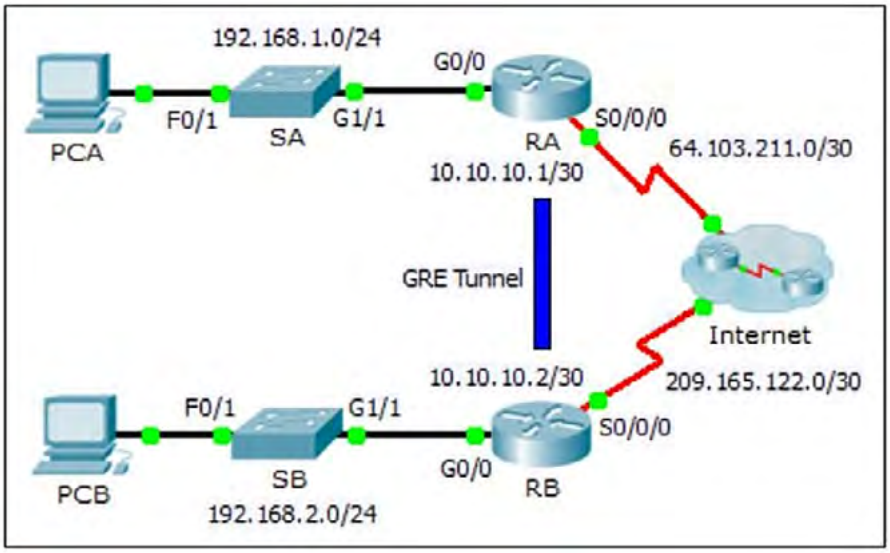
0								1								2								3							
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Versión				Clase de Tráfico								Etiqueta de Flujo																			
Longitud del campo de datos																				Cabecera siguiente								Límite de saltos			
Dirección de Origen																															
Dirección de Destino																															

Versión	4
Clase de tráfico (prioridad de paquete)	8
Etiqueta de flujo (calidad de servicio)	20
Longitud del campo de datos	16
Cabecera siguiente	8
Límite de saltos (tiempo de vida)	8
Dirección de origen	128
Dirección de destino	128
total	320

Fuente: elaboración propia.

En la Figura 38 se muestra el diagrama de transición IPv4 a IPv6.

Figura 38
Diagrama de Transición IPv4 a IPv6



Fuente: elaboración propia.

En la Tabla 58 se muestra la tabla de direccionamiento.

Tabla 58
Tabla de Direccionamiento

Device	Interface	IP Address	Subnet Mask	Default Gateway
RA	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	64.103.211.2	255.255.255.252	N/A
	Tunnel 0	10.10.10.1	255.255.255.252	N/A
RB	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	209.165.122.2	255.255.255.252	N/A
	Tunnel 0	10.10.10.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.2.2	255.255.255.0	192.168.2.1

Fuente: elaboración propia.

XXX. Configuraciones

MIKROTIK

Interface Generic Routing Encapsulation –GRE– es un protocolo de túnel desarrollado por Cisco en su origen. Es el mismo que IPIP y EoIP que fueron desarrollados originalmente como túneles sin estado lo que significa que si el extremo remoto del túnel se cae, todo el tráfico que se dirige a través de los túneles se convierte *blackholed*. Para resolver este problema, RouterOS han añadido característica "keepalive" para túneles GRE. Este túnel puede reenviar paquetes IP únicas e IPv6 (ethernet tipo 800 y 86dd). En la Tabla n.º 58 se observan los comandos a utilizar para generar el túnel GRE VPN.

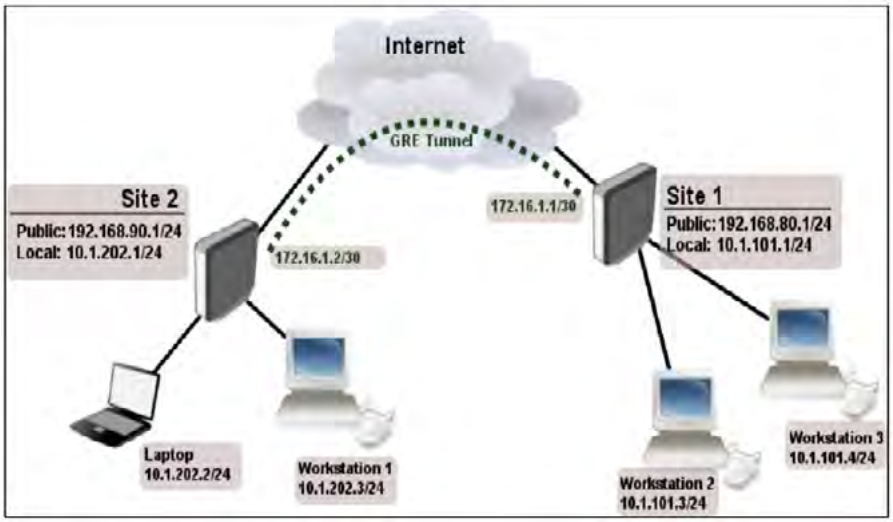
Tabla 59
Comandos GRE VPN

Propiedad	Descripción
comment (*string*; por defecto:)	Breve descripción del túnel.
disabled (*yes* | *no*; por defecto: no)	Activa / desactiva el túnel.
dscp (*heredar|entero[063]*; por defecto:)	Desde v5.6, dscp valor establecido en la cabecera GRE a un valor fijo o heredan de valor dscp tomado de tráfico tunelizado
keepalive (número *entero [1..4294967295]* ; defecto:)	Túnel keepalive tiempo de espera en segundos. Por keepalive por defecto está desactivada.
l2mtu (número *entero [0..65536]* ; defecto:65535)	Layer2 unidad de transmisión máxima.
local-address (*IP*; por defecto: 0.0.0.0)	Dirección IP que se utilizará para el extremo de túnel local. Si se establece en 0.0.0.0, se utilizará la dirección IP de la interfaz de salida.
mtu (número *entero [0..65536]* ; defecto:1476)	Layer3 unidad de transmisión máxima.
name (*string*; por defecto:)	Nombre del túnel.
remote-address (*IP*; por defecto:)	Dirección IP de extremo de túnel remoto.

Fuente: CISCO, 2008.

El objetivo es para obtener conectividad de Capa 3 entre dos sitios remotos a través de Internet, así como se puede observar en la Figura 39:

Figura 39
Capa 3 Túnel GRE



Fuente: CISCO, 2010

Se tienen dos sitios: Sitio1 con rango de red local 10.1.101.0/24 y Sitio2 con rango de red local 10.1.202.0/24.

El primer paso es la creación de túneles GRE. Router en el sitio 1:

/interfaz gre add name =gre ICA; remote-address=192.168.90.1; local-address= 192.168.80.1

Creación del túnel en el sitio 2:

/interface gre add name=gre CHICLAYO; remote-address=192.168.80.1; local-address=192.168.90.1

XXXI. Controles de seguridad principal en IPv6:

Seguridad en la Red: utilizar cortafuegos dedicados a los sistemas de cabecera independientes de más protegida de nuevo entornos de oficina. Los *firewalls* se han mejorado con políticas de seguridad IPv6 que responden a políticas IPv4 existentes tal como se observa en la Tabla 60.

Tabla 60
Seguridad en la red

Ancho de banda de tránsito	Ancho de banda de peering	Backbone
Estos enlaces se utilizan para el tráfico de producción y requieren tanto IPv4 como IPv6 conectividad de red a través de una infraestructura provider's	VeriSign maintalns 10G vincula en telas de peering en los sitios de resolución co-localización con conectividad IPv6-capaz en cada par	VeriSign pasa los paquetes IPv4 e IPv6 en longitudes de onda troncales dedicados que interconectan nuestros sitios de resolución y de aprovisionamiento. La columna vertebral fue diseñado desde el principio para ser preparado para IPv6.

Fuente: Verisign, 2012.

Dispositivos de Red: se encuentran en todos los puntos de conexión donde debe pasar IPv4 y paquetes IPv6 a velocidad de línea. Son capaces de mucho más que un paquete de enrutamiento. Para asegurar que el diseño no invoca rutinas de código que las hacen tasa de capacidad limitada, se requiere ser cuidadoso para no afectar de forma negativa el tráfico de impactos para ambos protocolos. A continuación, se muestra en la Tabla 61 los dispositivos de red servidores:

Tabla 61
Dispositivos de red servidores

Servidor de cabecera	Servidor de monitorización	Servidor de aplicaciones	Servidor de base de datos
Permite a cualquier host que termine la conexión a Internet, como por ejemplo un servidor de nombres o servidor web. Por lo tanto, estos servidores son por lo general en la primera línea para la accesibilidad de los clientes a IPv6	Estos sistemas dedicados que analizan el tráfico y los servicios también se amplía para monitorear IPv6	Algunos servidores de aplicaciones requieren conectividad IPv6 con el fin de realizar la validación de la transacción y cualquier otra forma de actuar sobre las solicitudes recibidas de los servidores de cabecera	Una dirección IPv6 es en esencia más grande que un IPv4 uno-28 bits comparados con 32 esto implica que el esquema de base de datos cambia cuando una dirección IP del cliente tiene que ser almacenado, como en el caso de los sistemas de aprovisionamiento de VeriSign

Fuente: Verisign, 2012.

Determinar el costo económico del diseño de controles de seguridad al usar IPv6 para recuperación de datos en caso de desastre en una entidad técnica privada.

En la Tabla 62 se muestra el flujo de caja del proyecto.

Tabla 62
Flujo de caja

Proyecto	Período cero	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.	Totales
INGRESOS								
PROGRAMA	S/. 23,225.00	S/. 9,800.00	S/. 10,500.00	S/. 10,500.00	S/. 10,500.00	S/. 10,500.00	S/. 10,500.00	S/. 85,525.00
Documentación	-	S/. 1,000.00	S/. 1,700.00	S/. 1,700.00	S/. 1,700.00	S/. 1,700.00	S/. 1,700.00	S/. 9,500.00
Mantenimiento SW	-	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 5,700.00
Mantenimiento HW	-	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 1,900.00	S/. 5,700.00
MATERIALES								
Papel bond A-4 75 gramos	S/. 72.00	-	-	-	-	-	-	S/. 72.00
Tinta Sistema Continuo Impresora	S/. 50.00	-	-	-	-	-	-	S/. 50.00
Folder manila.	S/. 30.00	-	-	-	-	-	-	S/. 30.00
Lapiceros PILOT BPS-GP (F)	S/. 27.00	-	-	-	-	-	-	S/. 27.00
EQUIPOS								
Laptop HP DV6707 US	S/. 1,800.00	-	-	-	-	-	-	S/. 1,800.00
Impresora Multifuncional F380	S/. 299.00	-	-	-	-	-	-	S/. 299.00
Servidor IBM System x3400 M3 X 2	S/. 6,691.00	-	-	-	-	-	-	S/. 6,691.00

IBM Server 1 TB 7200 SATA 3.5in HS	S/. 5,696.00	-	-	-	-	-	-	S/. 5,696.00
Memoria IBM 2GB (1x2GB) DDR3 1333MHz PC3-10600, ECC,	S/. 2,455.00	-	-	-	-	-	-	S/. 2,455.00
SWITCH CISCO SF300-48 PUERTOS	S/. 5,000.00	-	-	-	-	-	-	S/. 5,000.00
Mikrotik RB2011L-RM	S/. 405.00	-	-	-	-	-	-	S/. 405.00
SERVICIOS								
Movilidad y viáticos.	S/. 700.00	S/. 5,000.00	S/. 5,000.00	S/. 5,000.00	S/. 5,000.00	S/. 5,000.00	S/. 5,000.00	S/. 15,700.00
EGRESOS								
PERSONAL	-	S/. 18,000.00	S/. 18,000.00	S/. 18,000.00	S/. 18,000.00	S/. 18,000.00	S/. 18,000.00	S/. 108,000.00
Coordinador DRP TI		S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 48,000.00
Coordinador de Infraestructura tecnológica		S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 21,000.00
Coordinador de Sistema de Información		S/. 3,000.00	S/. 3,000.00	S/. 3,000.00	S/. 3,000.00	S/. 3,000.00	S/. 3,000.00	S/. 18,000.00
Coordinador de Seguridad de información		S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 3,500.00	S/. 21,000.00
Flujo de caja al mes	S/. 23,225.00	S/. 27,800.00	S/. 28,500.00	S/. 28,500.00	S/. 28,500.00	S/. 28,500.00	S/. 28,500.00	S/. 193,525.00

Fuente: elaboración propia.

En la Tabla 63 se muestra el ahorro ocasionado por el proyecto.

Tabla 63
Flujo de Ahorro

Ahorro	Jul. 2015	Ago. 2015	Sep. 2015	Oct. 2015	Nov. 2015	Dic. 2015	Total
Auxiliares documentación	S/. 9,000.00	S/. 9,000.00	S/. 9,000.00	S/. 9,000.00	S/. 9,000.00	S/. 9,000.00	S/. 54,000.00
Alquiler de laboratorio	S/. 20,000.00	S/. 20,000.00	S/. 20,000.00	S/. 20,000.00	S/. 20,000.00	S/. 20,000.00	S/. 120,000.00
Corriente eléctrica	S/. 5,000.00	S/. 5,000.00	S/. 5,000.00	S/. 5,000.00	S/. 5,000.00	S/. 5,000.00	S/. 30,000.00
Material de escritorio	S/. 2,500.00	S/. 2,500.00	S/. 2,500.00	S/. 2,500.00	S/. 2,500.00	S/. 2,500.00	S/. 15,000.00
Subtotales	S/. 36,500.00	S/. 36,500.00	S/. 36,500.00	S/. 36,500.00	S/. 36,500.00	S/. 36,500.00	S/. 219,000.00

Fuente: elaboración propia.

Se observa en la Tabla 64 el resumen de los flujos económicos.

Tabla 64
Resumen de los flujos económicos

Resumen de ahorro y costo	
Ahorro y beneficio total	S/. 219,000.00
Costo de implementar PY	S/. 193,525.00
Flujo de caja neto	S/. 25,475.00

Fuente: elaboración propia.

Ahora se realiza la rentabilidad, así como se contempla en la Tabla 65.

Tabla 65
Resumen de rentabilidad

Rentabilidad mensual requerida	10%
Vida útil de la inversión	6

Fuente: elaboración propia.

– Valor Actual Neto

Tabla 66
Flujo Económico Mensual

Flujos	PERÍODO CERO	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
		2015	2015	2015	2015	2015	2015	
Ahorros	0	S/. 36,500.00	S/. 36,500.00	S/. 36,500.00	S/. 36,500.00	S/. 36,500.00	S/. 36,500.00	S/. 219,000.00
Costos	S/. 23,225.00	S/. 27,800.00	S/. 28,500.00	S/. 28,500.00	S/. 28,500.00	S/. 28,500.00	S/. 28,500.00	S/. 193,525.00
Flujo Neto	-23,225	S/. 8,700.00	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 25,475.00
VAN	S/. 12,253.45							
TIR	27%							

Fuente: elaboración propia.

El valor actual neto sale **S/. 12,253.45**, lo que significa que el VAN es aceptable porque es superior a cero, así como se observa en la Tabla 67.

Tabla 67
Valor del VAN

VALOR	SIGNIFICADO	DECISIÓN A TOMAR
VAN > 0	La inversión produciría ganancias por encima de la rentabilidad exigida (r)	El proyecto puede aceptarse
VAN < 0	La inversión produciría pérdidas por debajo de la rentabilidad exigida (r)	El proyecto debería rehacerse
VAN = 0	La inversión no produciría ni ganancias ni pérdidas	Dado que el proyecto no agrega valor monetario por encima de la rentabilidad exigida (r), la decisión debería basarse en otros criterios, como la obtención de un mejor posicionamiento en el mercado u otros factores.

Fuente: elaboración propia.

– Tasa de interés de retorno

La tasa de interés de retorno sale **27%** mensual, lo que significa que el TIR es aceptable en el proyecto, tal como se observa en la Tabla 68.

Tabla 68
Valor del TIR

Si tir Se aceptará el proyecto. La razón es que el proyecto da una rentabilidad mayor que la rentabilidad mínima requerida (el coste de oportunidad).
Si tir Se rechazará el proyecto. La razón es que el proyecto da una rentabilidad menor que la rentabilidad mínima requerida.
Donde r representa rentabilidad propuesta por SENATI **10%**.

Fuente: elaboración propia.

– Beneficios de la Propuesta

Se muestran a continuación los beneficios cualitativos de la propuesta al utilizar como herramienta de análisis COBIT 4.1. En la Tabla 69 se muestra la continuidad del servicio con un cumplimiento del 70% (7 puntos).

Más tarde, se muestra en la Tabla 70 la seguridad de los sistemas con un cumplimiento del 89 % (25 puntos).

Por último, en la Tabla 71 se muestra Plan Estratégico TI con un cumplimiento del 91% (10 puntos).

Tabla 69
Beneficio de la propuesta DS4

	Evaluación	
DS4 Garantizar la Continuidad del Servicio	No Cumple	Cumple
DS4.1 Marco de Trabajo de Continuidad de TI		
Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias.		1
DS4.2 Planes de Continuidad de TI		
Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio.		1
DS4.3 Recursos Críticos de TI		
Puntos determinados como los más críticos en el Plan de Continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio		1
DS4.4 Mantenimiento del Plan de Continuidad de TI		
Exhortar a la Gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio.	1	
DS4.5 Pruebas del Plan de Continuidad de TI		
Probar el Plan de Continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable.		1
DS4.6 Entrenamiento del Plan de Continuidad de TI		
Asegurarse de que todos las partes involucradas reciban sesiones de habilitación de forma regular respecto a los procesos y sus roles y responsabilidades		1
	Evaluación	

DS4 Garantizar la Continuidad del Servicio	No Cumple	Cumple
DS4.7 Distribución del Plan de Continuidad de TI		
Determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas.	1	
DS4.8 Recuperación y Reanudación de los Servicios de TI		
Planear las acciones a tomar durante el período en que TI se recupera y reanuda los servicios. Esto puede representar la activación de sitios de respaldo.		1
DS4.9 Almacenamiento de Respaldo fuera de las Instalaciones		
Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio.		1
DS4.10 Revisión Post Reanudación		
Determinar si la Gerencia de TI ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.	1	
TOTAL	3	7

Fuente: elaboración propia.

Tabla 70
Beneficio de la propuesta DS5

	Evaluación	
DS5 Garantizar la seguridad de los sistemas	No Cumple	Cumple
DS5.1 Administración de la seguridad de TI		
Se administra la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.		1
DS5.2 Plan de seguridad de TI		
Se traslada los requerimientos de información del negocio y la configuración de TI a un plan global de seguridad de TI.		1
Se traslada los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI.		1
El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, *software* y *hardware*.		1
Las políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios.		1
DS5.3 Administración de identidad		
Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) son identificables de manera única.		1
Los derechos de acceso del usuario a sistemas y datos están alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo.		1
Los derechos de acceso del usuario son solicitados por la Gerencia del usuario.		1
Los derechos de acceso del usuario son aprobados por el responsable del sistema.		1
Los derechos de acceso del usuario son implementados por la persona responsable de la seguridad.		1
Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central.		1

Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.		1
DS5.4 Administración de cuentas del usuario		
Se garantiza que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, son tomados en cuenta por la Gerencia de cuentas de usuario.		1
Se incluye un procedimiento que describa al responsable de los datos o del sistema para otorgar los privilegios de acceso		1
Los procedimientos se aplican a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia		1
Los derechos y obligaciones relacionados al acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios.		1
La Gerencia lleva a cabo una revisión regular de todas las cuentas y los privilegios asociados.		1
DS5.5 Pruebas, vigilancia y monitoreo de la seguridad		
Se garantiza que la implementación de la seguridad en TI es probada y monitoreada de forma proactiva.		1
La seguridad en TI es reacreditada con regularidad para garantizar que se mantiene el nivel seguridad aprobado.	1	
Una función de ingreso al sistema y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención.		1
El acceso a la información de ingreso al sistema está alineado con los requerimientos del negocio en términos de requerimientos de retención y de derechos de acceso.		1
DS5.6 Definición de incidente de seguridad		
Se garantiza que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes	1	
DS5.7 Protección de la tecnología de seguridad		

Se garantiza que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que mantenga un perfil bajo.		1
La seguridad de los sistemas depende de la confidencialidad de las especificaciones de seguridad.		1
DS5.8 Administración de llaves criptográficas		
Se determina que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.	1	
DS5.9 Prevención, detección y corrección de software malicioso		
Se garantiza que se cuente con medidas de prevención, detección y corrección (en especial contar con parches de seguridad y control de virus actualizados) a lo largo de toda la organización para proteger a los sistemas de información y a la tecnología contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento desarrollado por dentro, etc.).		1
DS5.10 Seguridad de la red		
Se garantiza que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.		1
DS5.11 Intercambio de datos sensitivos		
Se garantiza que las transacciones de datos sensibles sean intercambiadas solo a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.		1
TOTAL	3	25

Fuente: elaboración propia.

Tabla 71
Beneficio de la propuesta P01

	Evaluación	
P01 Definir un Plan Estratégico de TI	No Cumple	Cumple
P01.1 Administración del Valor de TI		
El negocio es garantizar que el portafolio de inversiones de TI de la empresa contenga programas con casos de negocio sólidos. Reconocer que existen inversiones obligatorias, de sustento y discrecionales que difieren en complejidad y grado de libertad en cuanto a la asignación de fondos.		1
Los procesos de TI deben proporcionar una entrega efectiva y eficiente de los componentes TI de los programas y advertencias oportunas sobre las desviaciones del plan, incluyendo costo, cronograma o funcionalidad, que pudieran impactar los resultados esperados de los programas.		1
Establecer una evaluación de los casos de negocio que sea justa, transparente, repetible y comparable, incluyendo el valor financiero, el riesgo de no cumplir con una capacidad y el riesgo de no materializar los beneficios esperados.		1
P01.2 Alineación de TI con el Negocio		
Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el negocio para capitalizar esas oportunidades.		1
Las estrategias de negocio y de TI deben estar integradas, al relacionar de manera clara las metas de la empresa y las metas de TI y reconociendo las oportunidades, así como las limitaciones en la capacidad actual, y se deben comunicar de manera amplia.		1
Identificar las áreas en que el negocio (estrategia) depende de forma crítica de TI, y mediar entre los imperativos del negocio y la tecnología, de tal modo que se puedan establecer prioridades concertadas.		1
P01.3 Evaluación del Desempeño y la Capacidad Actual		
Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.	1	
P01.4 Plan Estratégico de TI		

Crear un Plan Estratégico que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados		1
El Plan Estratégico de TI debe incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de obtención, la estrategia de adquisición, y los requerimientos legales y regulatorios. El Plan Estratégico debe ser lo suficiente detallado para permitir la definición de Planes Tácticos de TI.		1
P01.5 Planes Tácticos de TI		
Los Planes Tácticos deben tener el detalle suficiente para permitir la definición de planes de proyectos. Administrar de forma activa los Planes Tácticos y las iniciativas de TI establecidas por medio del análisis de los portafolios de proyectos y servicios.		1
P01.6 Administración de Portafolio TI		
Administrar de forma activa, junto con el negocio, el portafolio de programas de inversión de TI requerido para lograr objetivos de negocio estratégicos específicos por medio de la identificación, definición, evaluación, asignación de prioridades, selección, inicio, administración y control de los programas.		1
TOTAL	1	10

Fuente: elaboración propia.

Conclusiones

- Se logró identificar, desarrollar, implementar y realizar prototipos para el establecimiento del proyecto, tales como el *tunneling* para la conexión VPN entre Ica y Chiclayo, herramientas IPER para evaluar los riesgos y desarrollar controles de seguridad IPv6.
- El Análisis de Impacto en el Negocio –BIA–, permitió el desarrollo de estrategias de continuidad de negocio para la recuperación de los recursos y procesos tales como SINFO, apertura de cursos y proceso de matrícula que son considerados como registros vitales; restaurar el servicio y proceso en un tiempo de 24 horas.
- La exposición de esta propuesta permitió que SENATI-Ica definiera, documentara y formalizara el 100% de las áreas críticas,

y estableciera los umbrales para los riesgos encontrados, permitiendo unificar criterios generales (basado en las normativas ISO 31000:2009, ISO 27001:2013, ISO 22301:2012) y específicos (políticas y procedimientos de seguridad).

- El manejo de las definiciones de los procesos a ejecutar en la gestión de riesgos permite manejar una herramienta IPER que ayuda al gestor a realizar un plan con un grado de asertividad del 95%, lo que otorgará certeza y agilidad de los procedimientos a realizar por el equipo del proyecto.
- Se logró identificar, mediante frecuencias y análisis de probabilidad e impacto, que cada diez años se manifiestan desastres naturales de gran magnitud (sobre todo inundaciones y terremotos), que afectan en un 30% los activos de SENATI-Ica.
- Es importante la participación constante y eficiente del equipo del proyecto para identificar, valorar y tratar todos los riesgos que puedan existir.
- IPv6 ofrece desafíos a todas las organizaciones, administradores responsables de proporcionar y apoyar los servicios en Internet. Las nuevas características de IPv6 acoplados con el estado de transición en el que IPv4 e IPv6 coexisten, dibujan un nuevo conjunto de medidas de seguridad que se establecen en particular en el despliegue de IPv6.
- La paridad funcional del servicio a través de los sistemas IPv4 e IPv6 separados, entregan un 80% de beneficio añadido para aislar funcionalidad y reducir las posibilidades de interrupción o degradación de los servicios durante el despliegue de IPv6.

Capítulo quinto
Reflexiones sobre el desarrollo del plan de recuperación de datos en caso de desastre mediante el protocolo IPv6

La implementación de mecanismo para la detención de fenómenos naturales (inundaciones, sismos u otros desastres), puede significar la capacidad no sólo en el campo de la ciencia, sino que además se estaría poniendo en el tapete asuntos de organización para el resguardo de la información entre otros aspectos de la vida y de la sociedad en general. Sin embargo, la investigación no fue en este sentido, el despliegue de la ciencia para determinar los grados de intensidad entre un fenómeno que pueda causar en el sistema social y desequilibrar los estamentos de organización entre ellos: sistemas operativos, datos de interés, manejo de la información que cada país pueda tener como parte de su control. En este aspecto, la mayoría de organizaciones a nivel mundial han deseado poseer como parte de su seguridad, sistemas que protejan en un sentido más amplio sus intereses, y con ellos, datos, informaciones de interés, entre otros aspectos. La aparición de eventos, momentos o circunstancias desfavorables que pudieran de alguna u otra manera desestructurar sus más preciados y por qué no sistemas operativos, lo cual traería como consecuencia la anulación permanente o total de su sistema operativo: cuestión que pondría en constante amenaza todo aquello que ha diseñado y puesto al servicio de sus usuarios.

Mucho se ha avanzado en este campo, aunque los desastres de cualquier índole se pueden prevenir, lo cierto es que en su totalidad esto aún no es una certeza, algunos países que pertenecen al "Cinturón de Fuego", que contempla una serie de regiones del pacífico sur han desarrollado un conjunto de acciones que pudieran dada la circunstancias de los desastres (también los tecnológicos), entre las actividades a de-

sarrollar estarían aquellas cuyo sistema de protección logrará minimizar el impacto que este evento trae consigo. Allí que la implementación de sistema IPv6, como protocolo de acción directa estaría delante para resguardar los distintos procedimientos y métodos que las organizaciones poseen.

Uno de los objetivos que se perseguía y, por ende, se logró sistematizar durante el desarrollo y ejecución del plan, era justo llevar a cabo un proyecto que permitiera recuperar los datos en el caso de desastre u otro evento que generara un descontrol y un posible colapso en el sistema operativo en sus organizaciones. Además de este objetivo central se desarrolló un método que consistió en evaluar las normativas relacionadas con el plan de recuperación de esos datos. De igual manera, identificar los protocolos alojados en el ciberespacio a fin de hacer una evaluación a posteriori, sobre la aparición de los distintos eventos o fenómenos naturales que lograran desestabilizar los datos que allí se encuentren.

Con la creación de una metodología que también se podría contemplar como un plan de emergencia se desarrolla un método que permitiera definir a grandes rasgos, formalizar en un 100% qué y dónde se alojan estas áreas definidas por los especialistas como críticas, y de esta manera, unificar los planes que las organizaciones estarían dispuestas a poner al servicio de la comunidad y la sociedad en general. Se trata de gestar un mecanismo que genere mayor grado de confiabilidad en los clientes, así como orientar a empresas a prestar mejores servicios al momento de presentarse de manera intempestiva momentos o circunstancias que pudieran sobrepasar la capacidad de respuesta de los sistemas y proveedores de servicios.

Desarrollar un Plan para la recuperación de datos bajo cualquier eventualidad que se haga presente puede minimizar cualquier impacto en ámbitos financieros, así como reducir, si fuera la situación, desastres que en otra época y bajo otro sistema de protección pudieran manifestarse. Sin un plan, la mayoría de las organizaciones no pudieran proteger sus intereses, tampoco generar entre sus usuarios niveles que confiabilidad a los fines de crear un clima de aceptabilidad, lo que significaría, también que los sistemas colapsaran y los controles de seguridad se vieran en su totalidad afectados so pena de crear un ambiente sospechoso en la posteridad.

La mayor parte de las organizaciones en aras de desarrollar niveles óptimos de confianza entre sus usuarios han visto que los desastres entendidos como fenómenos pueden desencadenar trastornos entre los miembros, así como situaciones que bien se pudieran evitar. Para ello, están los mecanismos de protección que son diseñados como parte de su ingeniería para salvaguardar los intereses económicos de un sinfín de organizaciones a nivel continental y mundial.

La puesta en marcha de un sistema de protección tal conocida como IPv6, propuesta que nace de la necesidad de proteger los sistemas operativos activos significa no solo el avance de las ciencias, sino que además permite el seguimiento bajo modalidad de estudio y de control sobre los acontecimientos que en un futuro pudiera afectar a la humanidad entera y con ella su garantía de seguridad. En este sentido, es bueno insistir en la necesidad irrebatible de que los países que sin parar afrontan los desequilibrios en materia no solo natural, sino tecnológicas puedan tomar sus previsiones a fin de contrarrestar las consecuencias que por lo general dejan estos fenómenos no solo afecta datos de interés, sino genera en el colectivo trastornos entre otras desavenencias, provocadas, de igual modo por negligencia u otra razón, aunque por lo general, los desastres provienen de situaciones u eventos que no pueden detectarse a tiempo.

Es de notar, que el desarrollo y puesto en funcionamiento de un plan como el IPv6 no garantiza en su totalidad la integridad del sistema, base de datos u otros servicios, sin embargo, este plan operativo puede contribuir a la detección de eventos que hace unos años era imposible determinar por la incipiente e inhóspita posibilidad de no contar con los avances de la ciencia y la tecnología.

Ahora, ¿por qué es tan importante contar con un sistema operativo o, dicho de otro modo, por qué es importante que las organizaciones tengan en su haber, una estructura tecnológica que las proteja de un inminente desastre.

Según las consideraciones de expertos cuando una compañía pierde o extravía por situaciones de fuerza mayor (inundaciones, colapso de las líneas eléctricas, tsunamis, tornados, sismos de alto impacto, o los desastres tecnológicos, hacker, intromisiones de terceros), no solo está poniendo en riesgo la información u otros materiales de interés, sino que está en amenaza criterios que opacarían su prestigio, rentabilidad

y un futuro promisorio en el ámbito competitivo: cuestión vital en toda organización.

Los sistemas de seguridad, al igual que los de información están sujetos a acciones vulnerables; tanto desde adentro como desde afuera de su sistema. Los llamados riesgos lógicos, que parten ante todo desde la permanente y acechante negación del propio sistema para acceder a sus dominios parecen obedecer a procesos mucho más complejos. De allí entender que no solo basta con desarrollar planes o sistemas que protejan de manera expedita la información que suelen almacenarse en los programas, sino que, de igual manera, se hace necesario saber los niveles de riesgos que corren las organizaciones, empresas y estados cuando no se posee un mecanismo de seguridad óptimo y confiable. En este sentido, ya no solo hablaríamos de fenómenos que ultrajan los sistemas operativos, sino que los desastres también pueden ser provocados por macro sistemas o dispositivos de inteligencia artificial que son diseñados por enormes consorcios financieros que vulneran otros sistemas de seguridad también superiores.

El plan IPv6, como método, además de tener como principal rol proteger los sistemas operativos de gran importancia para las organizaciones, también ha servido de plataforma para la detección de aspectos que tienen que ver con las acciones económicas de gran impacto. De igual modo, permitió analizar con mayor precisión el estudio sistemático de datos en diversas áreas consideradas como críticas. A su vez que este plan también podría servir de referente para el seguimiento de situaciones de desastres naturales, también aquellos provocados por negligencia y el comportamiento irresponsable y desmedido de funcionarios. De esta manera, la implementación de un protocolo de seguridad generaría al interior de las organizaciones el acápite de un sistema que logrará determinar sucesos o eventos que pudieran poner en riesgo los mecanismos necesarios para el mejoramiento de los servicios entre otros beneficios que están recibiendo las compañías en materia de telecomunicaciones quienes se han visto en la necesidad imperiosa de poner bajo este plan de seguridad toda su plataforma para un mejor desempeño.

Bibliografía

ACT. *ACT Government.*, 2014, disponible en [https://www.legislation.act.gov.au/a/2014-24/].

Alexander Servat, Alberto. *Gestión del Riesgo en el Business Continuity Planning*, Lima, 2006, disponible en [https://docplayer.es/2838466-Gestion-del-riesgo-en-el-business-continuity-planning.html#download_tab_content].

Alexander Servat, Alberto. *Nuevo Estándar Internacional en Continuidad del Negocio ISO 22301:2012*, Santo Domingo, República Dominicana, Torre Piantini, 2012, disponible en [http://www.gestion.com.do/pdf/018/018-nuevo-estandar-internacional.pdf].

Casarero, Eduardo; Alejandro Clemente y Santiago Ruiz. *IPV6*, Buenos Aires, Universidad Argentina de la Empresa, 2011, disponible en [https://docplayer.es/2097861-Ipv6-casarero-eduardo-clemente-alejandro-ruiz-santiago-universidad-argentina-de-la-empresa.html].

cisco. *IPV6 Addressing White Paper*, San Jose CA, EE. UU., 2008, disponible en [https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/IPv6_WP.pdf].

CISCO. *Testing IPV4*, 2017, disponible en [https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/performance-comparisons.pdf?dtid=osscdc000283]

CISCO. *Certificado PKI*, 2011, disponible en [https://www.cisco.com/c/en/us/td/docs/ios/sec_secure_connectivity/configuration/guide/12_2sr/sec_secure_connectivity_12_2sr_book/sec_store_pki_cred.pdf?dtid=osscdc000283].

CISCO. *Libros IPV6*, 2017, disponible en [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book/ip6-addrg-bsc-con.html?dtid=osscdc000283].

CISCO. *Usando GRE*, 2018, disponible en [https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/118361-technote-gre-00.html?dtid=osscdc000283].

COMPUTERWORLD. *Una de cada tres empresas españolas carece de planes de recuperación ante desastres*, 2011, disponible en [http://staging.computerworld.es/archive/una-de-cada-tres-empresas-espanolas-carece-de-planes-de-recuperacion-ante-desastres].

CONSULTING, A. *Controles Generales TI*, 2013.

EL PERUANO. *Ley n.º 29733 Ley Protección de Datos Personales*, Lima, Congreso de la República del Perú, 2011, disponible en [https://diariooficial.elperuano.pe/pdf/0036/ley-proteccion-datos-personales.pdf].

GOBIERNO REGIONAL DE ICA. *Plan Regional de Prevención y Atención de Desastres Región Ica 2009-2019*, Ica, 2009, disponible en [https://www.paho.org/per/index.php?option=com_docman&view=download&alias=219-plan-regional-preven-

cion-atencion-desastres-region-ica-2009-2019-9&category_slug=planes-procedimientos-protocolos-945&Itemid=1031].

IBM. *Servicios de Continuidad de Negocio*, 2014, disponible en [http://www-935.ibm.com/services/pe/es/it-services/servicios-de-continuidadde-negocio.html].

ICA, G. R. *Plan Atención de Desastre 2009-2019*, Ica, GORE, 2009, disponible en [https://www.paho.org/per/index.php?option=com_docman&view=download&alias=219-plan-regional-prevencion-atencion-desastres-region-ica-2009-2019-9&category_slug=planes-procedimientos-protocolos-945&Itemid=1031].

ICONTEC. *Norma técnica colombiana*, Colombia, ISO, 2013, disponible en [https://colaboracion.dnp.gov.co/CDT/Normograma/NTC-ISO%2030300%20de%202013.pdf].

INDECI. *Desastres naturales*, Ica, INDECI, 2011, disponible en [https://www.indeci.gob.pe/wp-content/uploads/2019/01/comp_2011.pdf].

INEI. *Compendio Estadístico Ica*, Ica, ODEI Ica, 2013, disponible en [https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib0967/libro.pdf].

LASPROVINCIAS.ES. *Las empresas no se preparan para hacer frente a un desastre*, 2006, disponible en [http://www.lasprovincias.es/valencia/pg060507/prensa/noticias/Economia/200 605/07/VAL-ECO-286.html].

MÉNDEZ JIMÉNEZ, GENARO. *Plan de Recuperación De Desastres Del Sistema SAP Considerando Falla en el Servidor Aplicativo de un Laboratorio Farmacéutico*, México, D. F., 2012, disponi-

ble en [http://132.248.52.100:8080/xmlui/bitstream/handle/132.248.52.100/2881/Tesis.pdf?sequence=1].

PECB. *ISO 22301*, 2012, disponible en [http://pecb.org/iso22301/].

PERÚ, I. G. *Desastres Naturales*, Nacional, IGP, 2013.

ROJAS, A. *Continuidad de negocio: Estrategias de Respaldo Recuperación ante Desastres*, diciembre de 2011.

SALAZAR, J. *Guía para crear un Plan de Recuperación en caso de desastre en el Sistema Informático del Centro de Datos de un Grupo Financiero*, San José, Costa Rica, 2008.

SMART, B. S. *Una visión general del proceso de Planificación de Recuperación de Desastres - de principio a fin*, 1999.

TECHTARGET. *Tecnologías actuales de respaldo y recuperación de datos con protección continua de datos (CDP)*, 2009, disponible en [https://searchdatacenter.techtarget.com/es/noticias/2240170035/Tecnologias-actuales-de-respaldo-y-recuperacion-de-datos-con-proteccion-continua-de-datos-CDP].

TRINEXUS TECHNOLOGIES. *Conceptos Básicos*, 2011, disponible en [http://www.consulintel.es/Html/Tutoriales/Trinexus/routing.htm].

WENKEL, ROLF. *Superado el impacto: la economía tras el 11-S*, 2006, disponible en [http://www.dw.de/superado-elimpacto-la-econom%C3%ADa-tras-el-11-s/a-2170235].

El autor

Cesar Augusto Cabrera García
cabreracesar092@gmail.com

Magister en Ingeniería de Seguridad Informática especializado en las normativas ISO 27001-SGSI y COBIT para marcos normativos de seguridad de la información en empresas. Ingeniero de Sistemas especializados en redes y servidores, certificado en CISCO IT ESSENTIALS, CCNNA. Actualmente es investigador principal del proyecto de investigación Energía Renovable 2018-2019 en el directorio de investigadores n.º 76139 CTI VITAE CONCYTEC - REGION ICA y docente ordinario auxiliar tiempo completo de la facultad de ingeniería - escuela profesional de ingeniería de computación y sistemas de la Universidad Privada San Juan Bautista.

Editado por el Instituto Latinoamericano de Altos Estudios –ILAE–,
en marzo de 2021

Se compuso en caracteres Cambria de 12 y 9 ptos.

Bogotá, Colombia