Seguridad y Administración del DATA CENTER

CONCEPTOS GENERALES

- INFRAESTRUCTURA
- DISTRIBUCIÓN
- REFRIGERACIÓN

INFRAESTRUCTURA

CONTEMPLACIÓN EN EL DISEÑO

- DISTRIBUCIÓN FÍSICA
- CAPACIDAD ELÉCTRICA
- REFRIGERACIÓN
- RESILIENCIA (backup de componentes)
- SEGURIDAD FÍSICA, CONTROL DE ACCESO

CONTEMPLACIÓN EN EL DISEÑO

- PATRONES DE USO (CPU intensive, storage intensive, etc.)
- CAPACIDAD DE CRECIMIENTO
- OPERATIVA Y COSTES (TCO)
- EQUIPOS DE APOYO

REFRIGERACIÓN

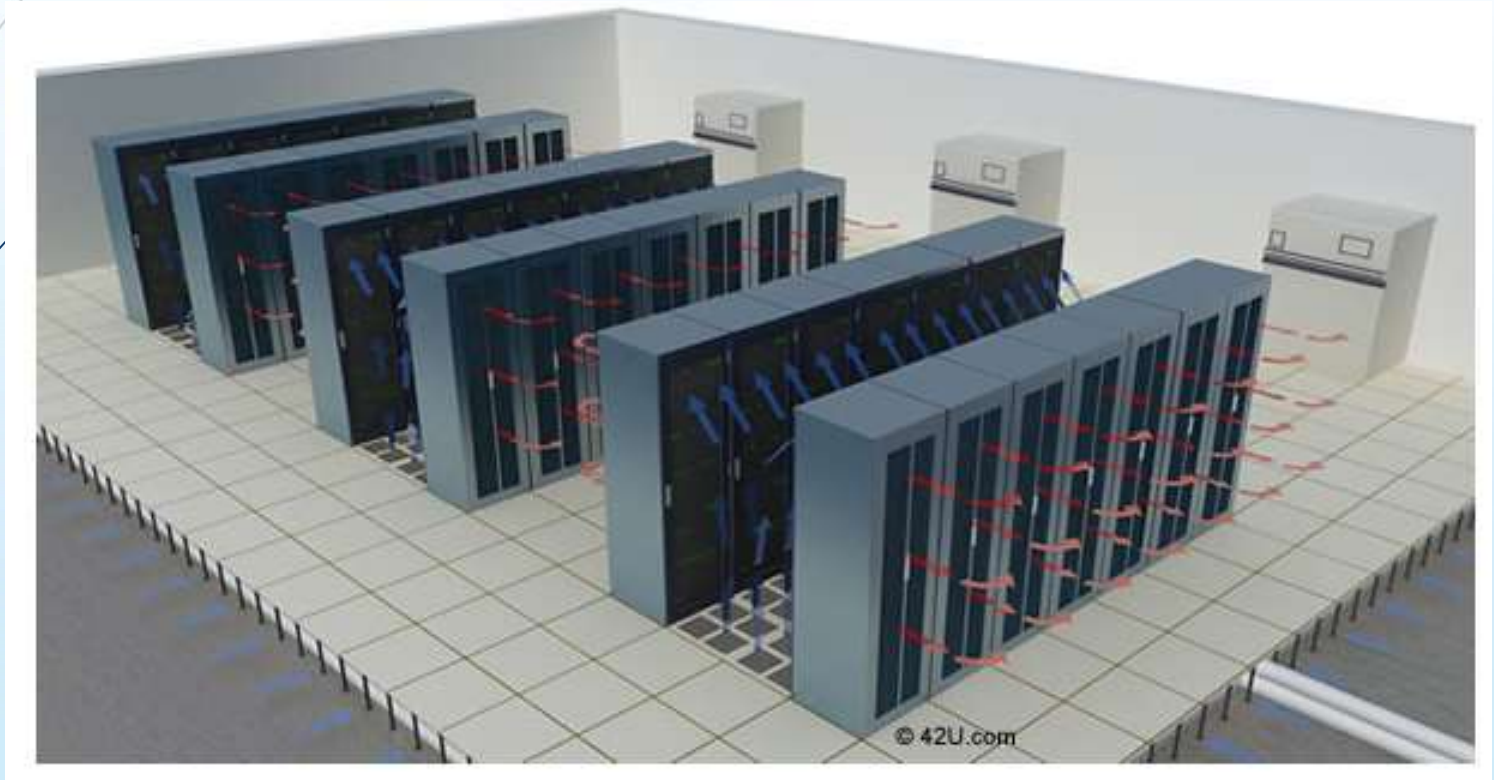
ELEMENTOS

- ENFRIADORAS, INDOOR-OUTDOOR
- CRAC / Aire Acondicionado
- CONDUCCIÓN/CIRCULACIÓN DE AIRE

CONSIDERACIONES A TENER EN CUENTA

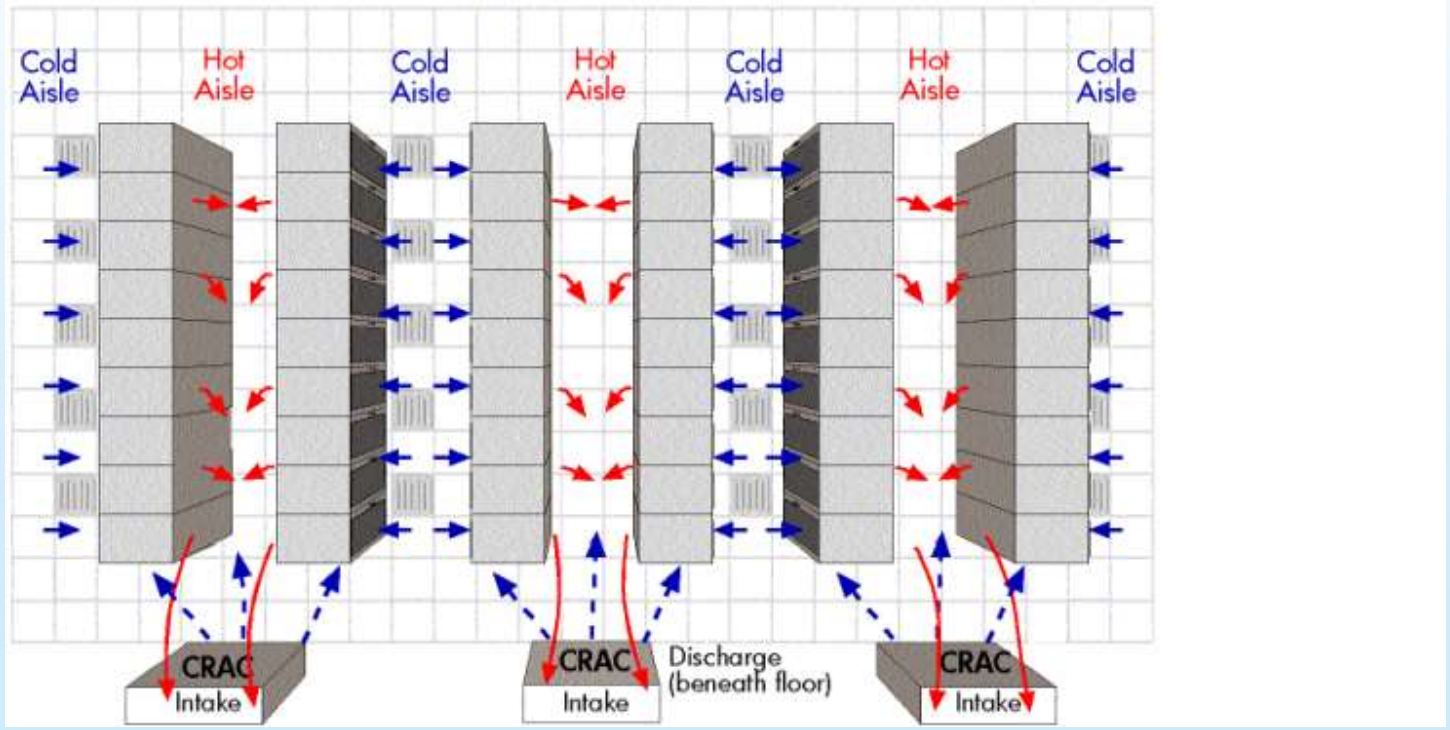
- SEPARACIÓN DE FLUJOS DE AIRE FRÍO Y CALIENTE
- DISTRIBUCIÓN ADECUADA

DISPOSICIÓN GENERAL DE UN DATACENTER



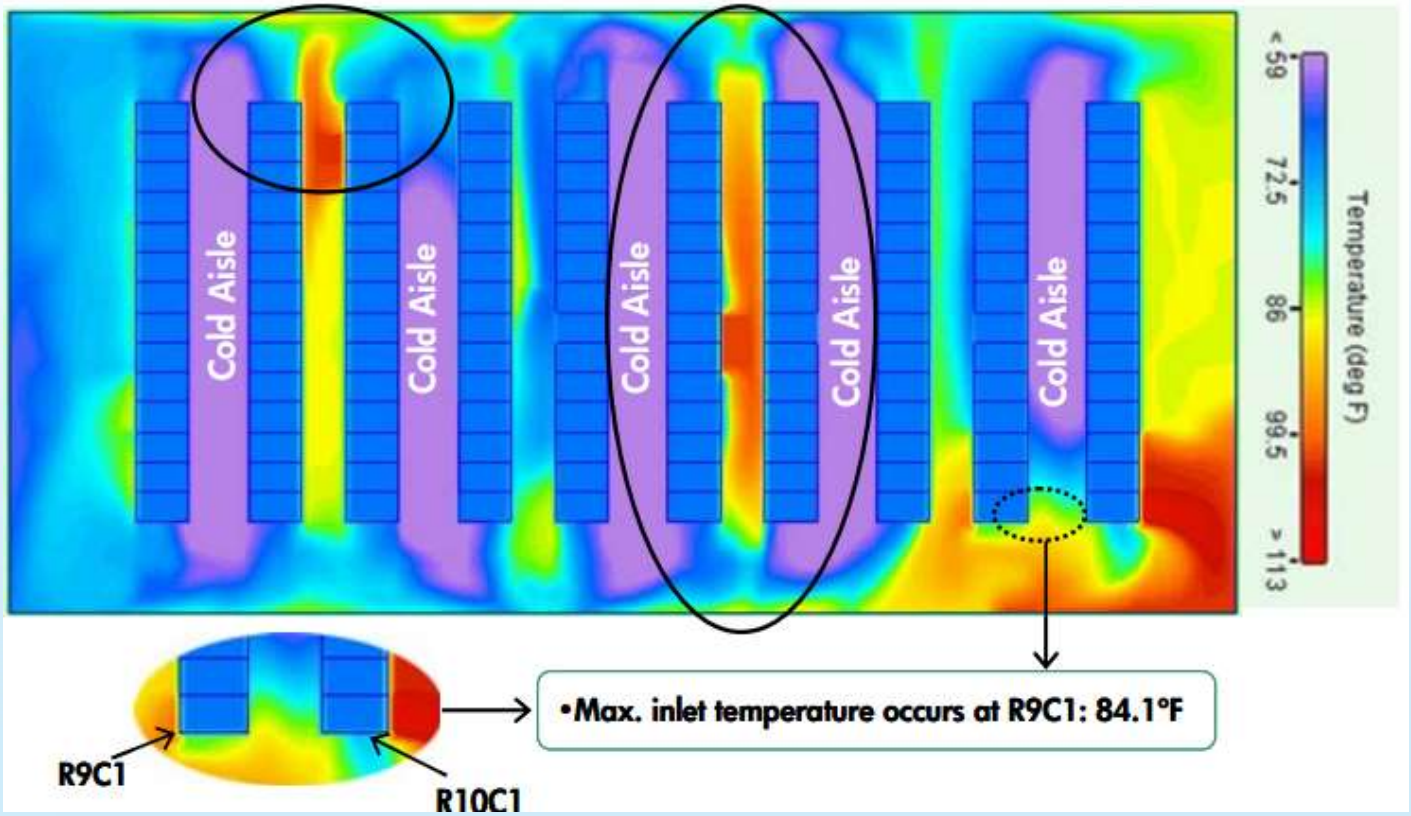
SEPARACIÓN DE FLUJOS DE AIRE

Figure 16. CRAC units should be placed perpendicular to hot aisles so that they discharge cool air beneath the floor in the same direction.



DISTRIBUCIÓN ADECUADA

Figure 14. Exhaust from the high-density rack wrapping around the end of the row



RESILIENCIA

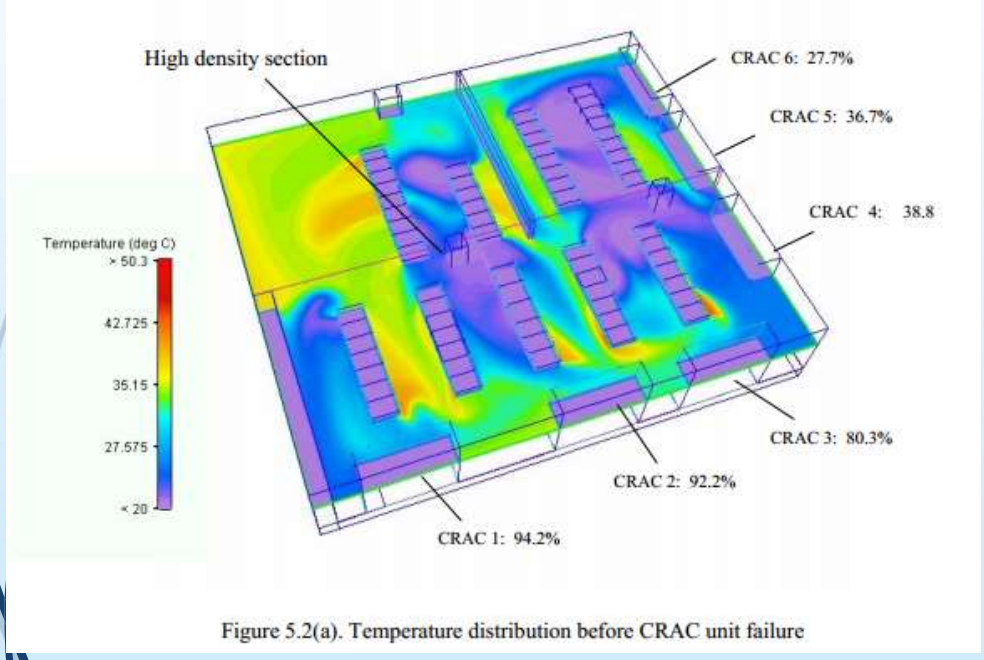


Figure 5.2(a). Temperature distribution before CRAC unit failure

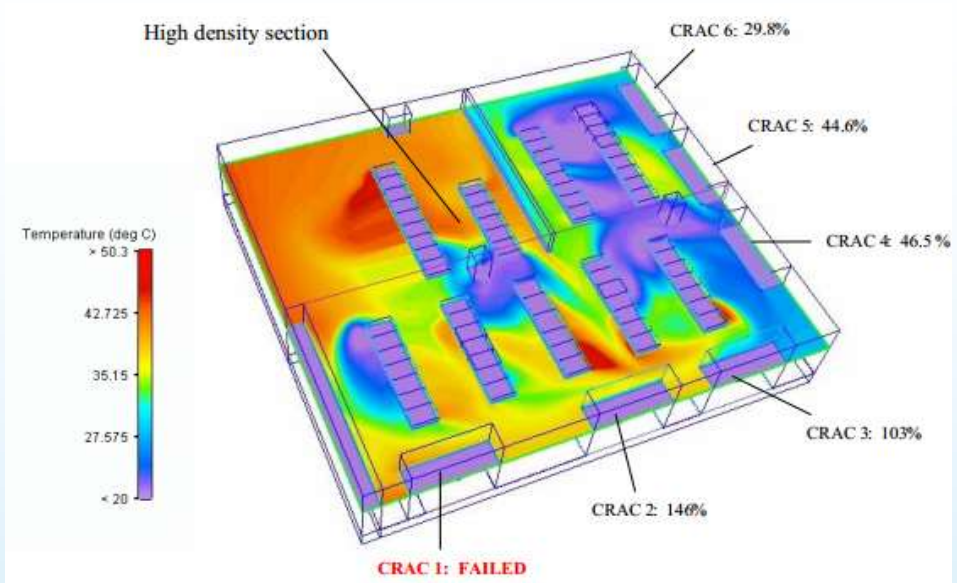
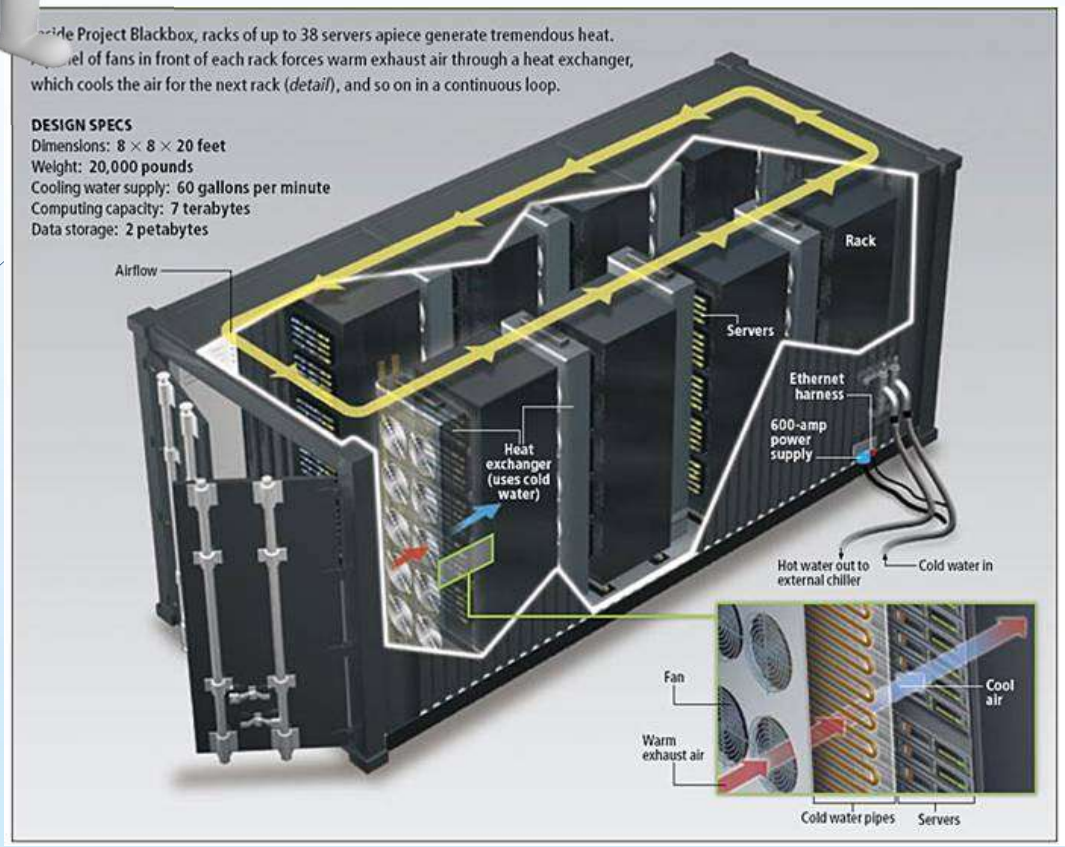


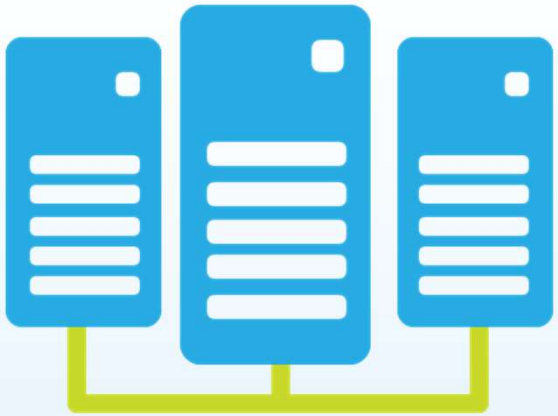
Figure 5.2. (b) Temperature distribution after CRAC unit failure.

DATO CURIOSO…



OTRAS CONTINGENCIAS

- SISTEMAS DE EXTINCIÓN DE INCENDIOS
- REDUNDANCIA DE SISTEMAS (generador, UPS, equipos de comunicaciones)
- REDUNDANCIA DE SUMINISTROS (acometida eléctrica, red)
- SEGURIDAD FÍSICA
- SEGURIDAD CONTRA INTRUSIONES INFORMÁTICAS
- SISTEMAS DE BACKUP (datos, configuraciones, etc.)
- PROTOCOLOS DE MANTENIMIENTO Y OPERACIÓN



GESTIÓN DEL DATACENTER

NORMATIVA EIA/TIA 942

ANSI/TIA-942-2005
Approved: April 12, 2005

TIA STANDARD

Telecommunications Infrastructure Standard for Data Centers

TIA-942

April 2005

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Representing the telecommunications industry in association with the Electronic Industries Alliance

Electronic Industries Alliance

ESTANDAR TIA 942

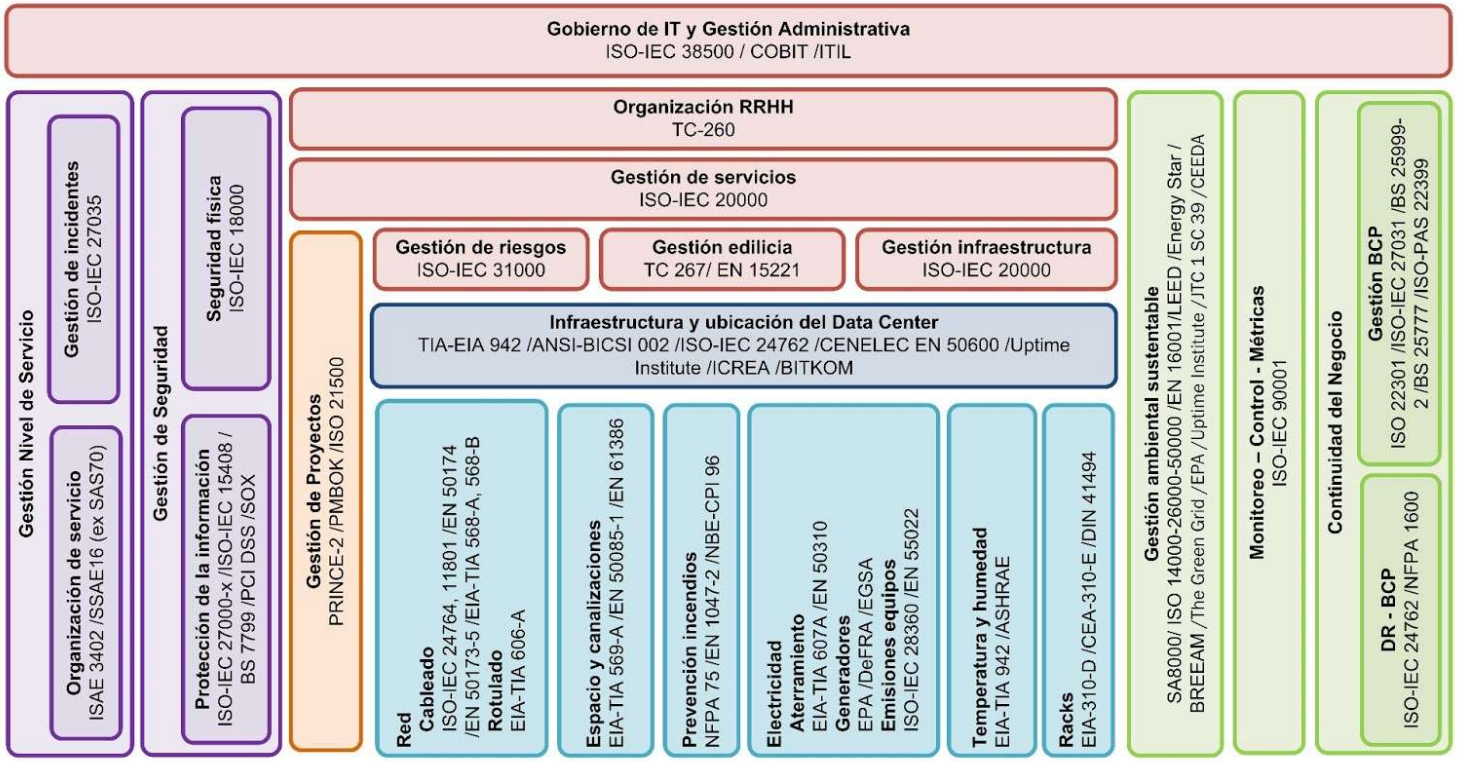
PROVEE UNA SERIE DE RECOMENDACIONES Y DIRECTRICES, PARA EL DISEÑO E INSTALACIÓN DE INFRAESTRUCTURAS DE DATA CENTERS.

LA INTENCIÓN ES QUE SEA UTILIZADO POR LOS DISEÑADORES QUE NECESITAN UN CONOCIMIENTO ACABADO DE LOS SERVICIOS DE PLANIFICACIÓN, EL SISTEMA DE CABLEADO Y EL DISEÑO DE REDES.

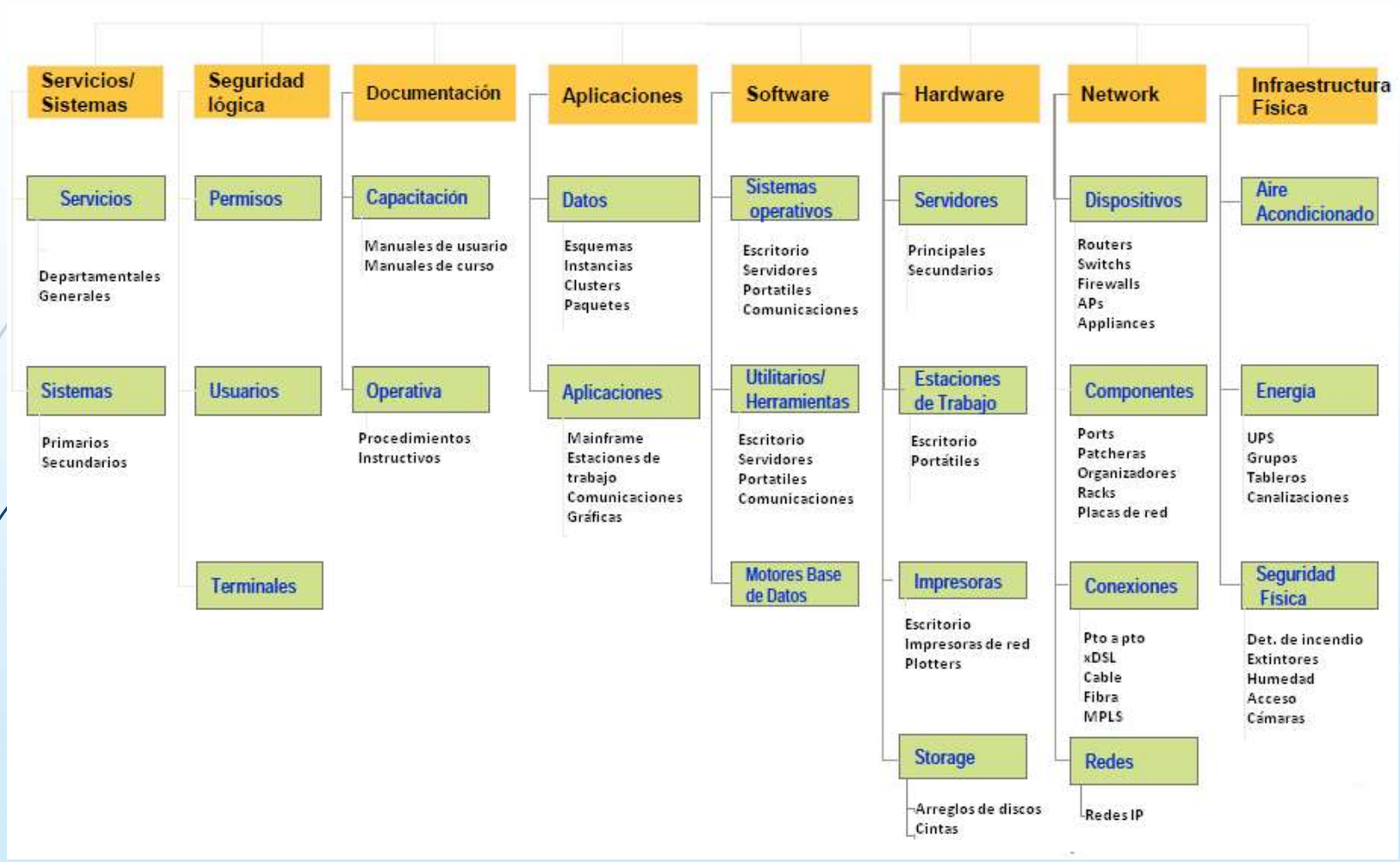
VENTAJAS DEL DISEÑO DE CENTROS DE DATOS DE CONFORMIDAD CON LA NORMA TIA 942:

- NOMENCLATURA ESTANDAR
- FUNCIONAMIENTO A PRUEBA DE FALLOS
- SÓLIDA PROTECCIÓN CONTRA CATÁSTROFES NATURALES O MANUFACTURADOS
- FIABILIDAD A LARGO PLAZO
- CAPACIDAD DE EXPANSIÓN Y ESCALABILIDAD

Estándares en el Data Center

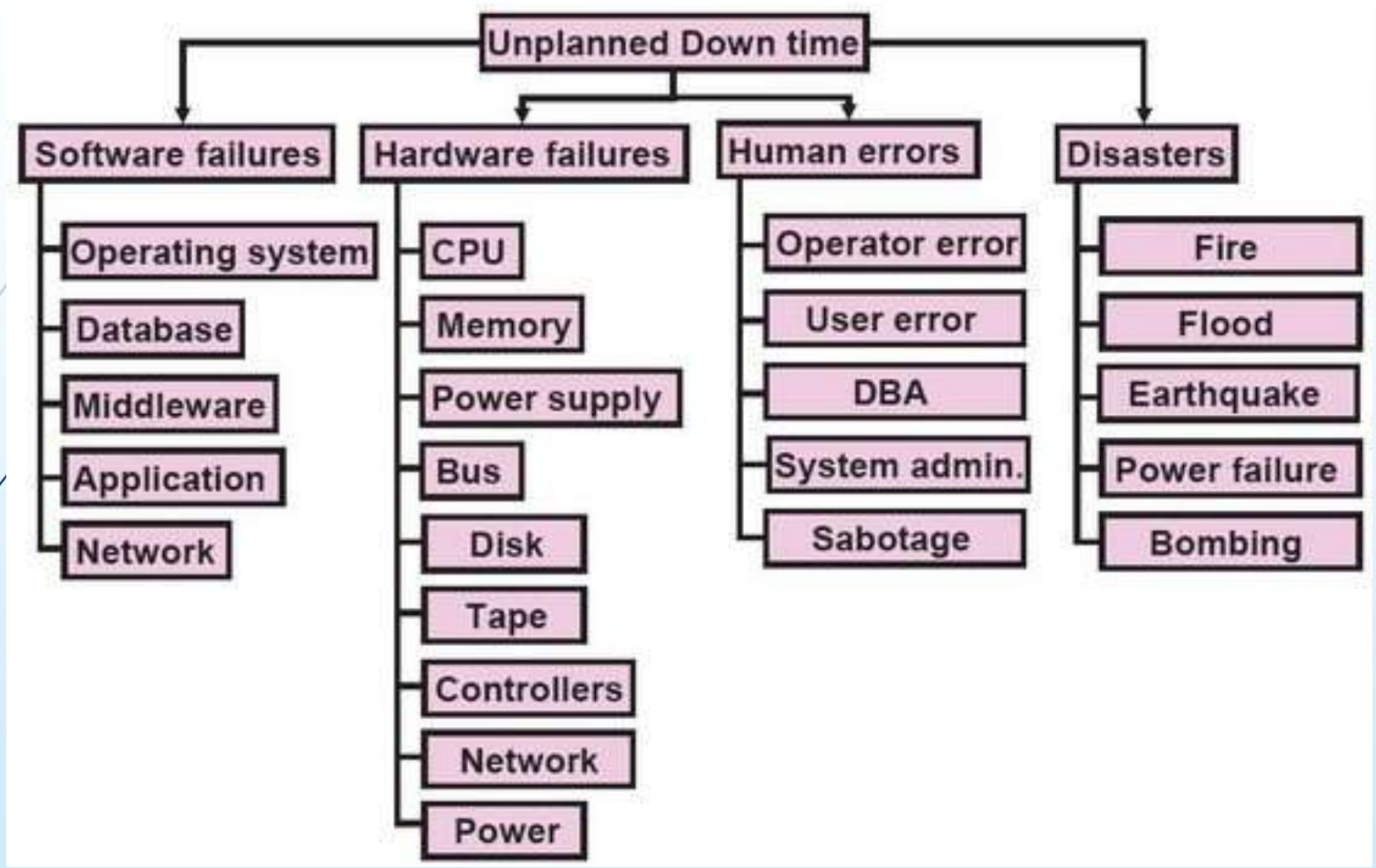


Los gráficos de burbujas representan subdivisiones por módulos agrupadas por color según el área de aplicación, en letra negrita se pueden el nombre de cada módulo o subdivisión. Los números representan los más estándares o Frameworks más importantes para ese módulo en particular.

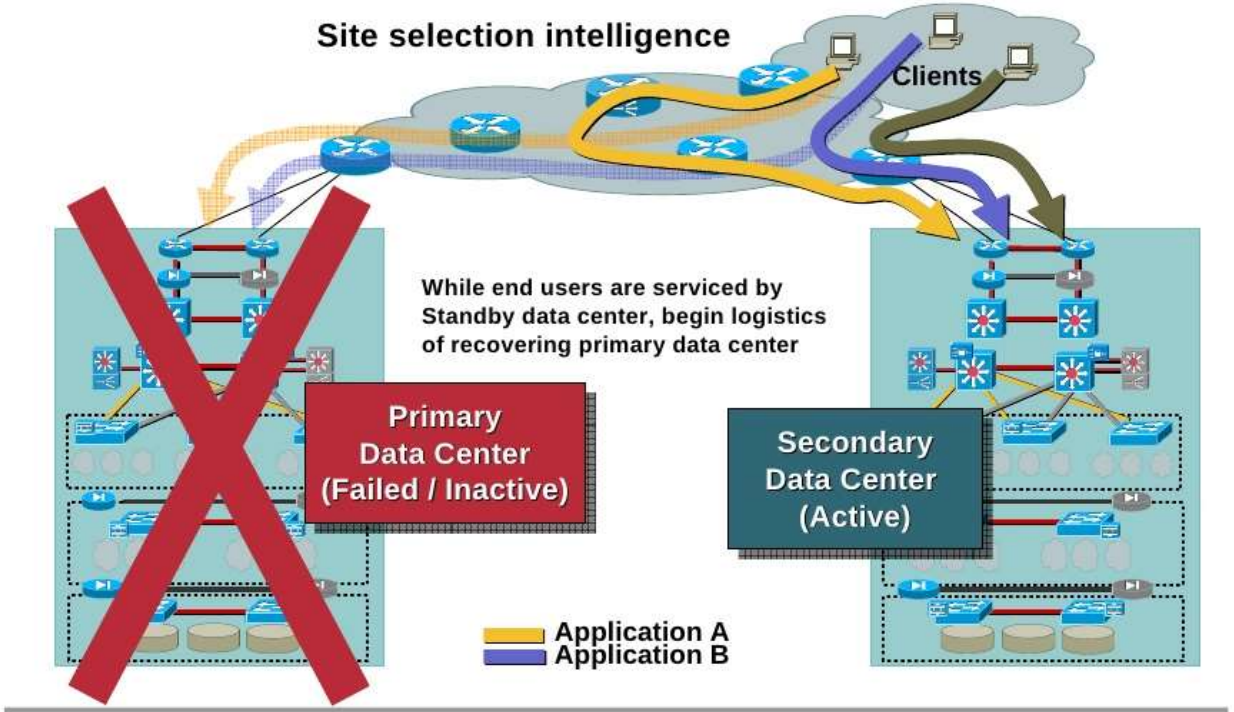

Servicios/ Sistemas
Servicios
Departamentales
Generales
Sistemas
Primarios
Secundarios
Seguridad lógica
Permisos
Usuarios
Terminales
Documentación
Capacitación
Manuales de usuario
Manuales de curso
Operativa
Procedimientos
Instructivos
Aplicaciones
Datos
Esquemas
Instancias
Clusters
Paquetes
Aplicaciones
Mainframe
Estaciones de trabajo
Comunicaciones
Gráficas
Software
Sistemas operativos
Escritorio
Servidores
Portatiles
Comunicaciones
Utilitarios/ Herramientas
Escritorio
Servidores
Portatiles
Comunicaciones
Motores Base de Datos
Hardware
Servidores
Principales
Secundarios
Estaciones de Trabajo
Escritorio
Portátiles
Impresoras
Escritorio
Impresoras de red
Plotters
Storage
Arreglos de discos
Cintas
Network
Dispositivos
Routers
Switchs
Firewalls
APs
Appliances
Componentes
Ports
Patcheras
Organizadores
Racks
Placas de red
Conexiones
Pto a pto
xDSL
Cable
Fibra
MPLS
Redes
Redes IP
Infraestructura Física
Aire Acondicionado
Energia
UPS
Grupos
Tableros
Canalizaciones
Seguridad Física
Det. de incendio
Extintores
Humedad
Acceso
Cámaras

OBJETIVO

EVITAR EL DOWNTIME


Unplanned Down time
Software failures
Operating system
Database
Middleware
Application
Network
Hardware failures
CPU
Memory
Power supply
Bus
Disk
Tape
Controllers
Network
Power
Human errors
Operator error
User error
DBA
System admin.
Sabotage
Disasters
Fire
Flood
Earthquake
Power failure
Bombing

Disaster Recovery
Hot Standby



SEGURIDAD FÍSICA Y LÓGICA DEL DATACENTER

SEGURIDAD DE LA INFORMACIÓN

LA INFORMACIÓN ES UN ACTIVO ESENCIAL PARA EL NEGOCIO DE UNA ORGANIZACIÓN, POR ENDE NECESITA SER PROTEGIDO ADECUADAMENTE

LA INFORMACIÓN PUEDE EXISTIR EN MUCHAS FORMAS:

- IMPRESA O ESCRITA EN UN PAPEL
- ALMACENADA ELECTRÓNICAMENTE
- TRANSMITIDA POR CORREO O UTILIZANDO MEDIOS ELECTRÓNICOS
- MOSTRADA EN PELÍCULAS O HABLADA EN UNA CONVERSACIÓN.

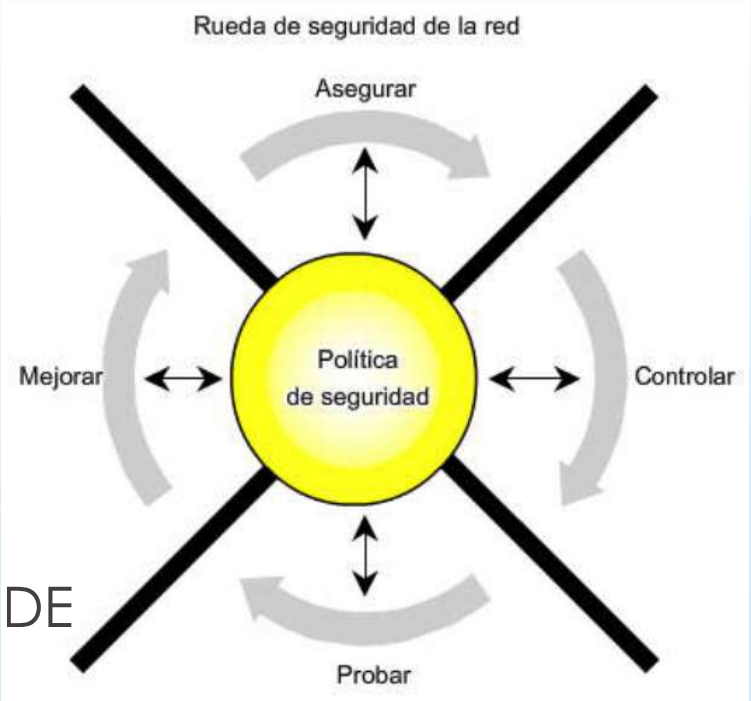
SEGURIDAD DE LA INFORMACIÓN

CUALQUIERA QUE SEA LA FORMA QUE TOME LA INFORMACIÓN, O MEDIO POR EL CUAL SEA ALMACENADA O COMPARTIDA, SIEMPRE DEBERÁ ESTAR APROPIADAMENTE PROTEGIDA

SEGURIDAD DE LA INFORMACIÓN

SE LOGRA IMPLEMENTANDO UN ADECUADO CONJUNTO DE CONTROLES, INCLUYENDO POLÍTICAS, PROCESOS, PROCEDIMIENTOS, ESTRUCTURAS ORGANIZACIONALES Y FUNCIONES DE SOFTWARE Y HARDWARE.

SE NECESITA ESTABLECER, IMPLEMENTAR, MONITOREAR, REVISAR Y MEJORAR ESTOS CONTROLES CUANDO SEA NECESARIO, PARA ASEGURAR QUE SE CUMPLAN LOS OBJETIVOS DE SEGURIDAD Y COMERCIALES ESPECÍFICOS.



REQUERIMIENTOS DE SEGURIDAD

ANALISIS DE RIESGO

- IDENTIFICAR REQUERIMIENTOS DE SEGURIDAD
- IDENTIFICAR Y DOCUMENTAR LOS RECURSOS QUE DEBEN PROTEGERSE
- IDENTIFICAR LA INFRAESTRUCTURA DE LA RED CON MAPAS E INVENTARIOS ACTUALES

EVALUACIÓN DE RIESGOS DE LA SEGURIDAD

LOS REQUERIMIENTOS DE SEGURIDAD SE IDENTIFICAN MEDIANTE UNA EVALUACIÓN METÓDICA DE LOS RIESGOS DE SEGURIDAD.

LOS RESULTADOS DE LA EVALUACIÓN DE RIESGO AYUDARÁN A GUIAR Y DETERMINAR LA ACCIÓN DE GESTIÓN APROPIADA Y LAS PRIORIDADES PARA MANEJAR LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, E IMPLEMENTAR CONTROLES SELECCIONADOS PARA PROTEGERSE CONTRA ESOS RIESGOS.

LA EVALUACIÓN DEL RIESGO DEBIERA REPETIRSE PERIODICAMENTE PARA TRATAR CUALQUIER CAMBIO QUE PUDIERA INFLUIR EN LOS RESULTADOS DE LA MISMA.

SELECCIÓN DE CONTROLES

UNA VEZ REALIZADA LA IDENTIFICACION DE REQUERIMIENTOS
Y RIESGOS DE SEGURIDAD Y TOMADAS LAS DECISIONES PARA EL TRATAMIENTO DE LOS RIESGOS, DEBEN SELECCIONARSE E IMPLEMENTARSE LOS CONTROLES APROPIADOS, ASEGURANDO QUE LOS RIESGOS SE REDUZCAN A UN NIVEL ACEPTABLE.

PUNTO DE INICIO DE LA SEGURIDAD DE LA INFORMACIÓN

SE PUEDEN CONSIDERAR UN NÚMERO DE CONTROLES

COMO UN BUEN PUNTO DE INICIO PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

ESTOS SE BASAN EN REQUERIMIENTOS LEGISLATIVOS ESENCIALES O PUEDEN SER CONSIDERADOS COMO UNA PRÁCTICA COMÚN PARA LA SEGURIDAD DE LA INFORMACIÓN.

SEGURIDAD FÍSICA

- ACCESO FÍSICO
- CONTROL DE TEMPERATURA Y HUMEDAD
- MONITOREO Y ALARMAS

SEGURIDAD LÓGICA

- CONTROL DEL FLUJO
- PERMISOS DE USUARIO
- MONITOREO Y ALARMAS

ÁREAS SEGURAS

OBJETIVO:

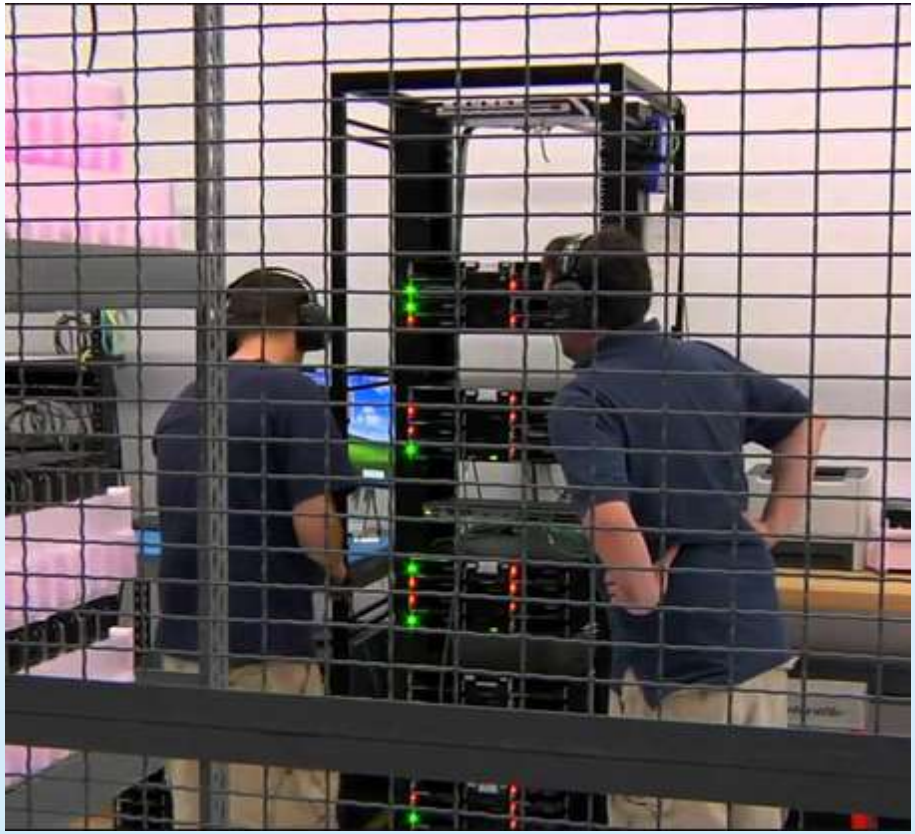
EVITAR EL ACCESO FÍSICO NO AUTORIZADO, DAÑO E INFERENCIA CON LA INFORMACIÓN Y LOS LOCALES DE LA ORGANIZACIÓN.

LOS MEDIOS DE PROCESAMIENTO DE INFORMACIÓN CRÍTICA O CONFIDENCIAL DEBIERAN UBICARSE EN ÁREAS SEGURAS, PROTEGIDAS POR LOS PERÍMETROS DE SEGURIDAD DEFINIDOS, CON LAS BARRERAS DE SEGURIDAD Y CONTROLES DE ENTRADA APROPIADOS. DEBIERAN ESTAR FÍSICAMENTE PROTEGIDOS DEL ACCESO NO AUTORIZADO, DAÑO E INTERFERENCIA.

PERÍMETRO DE SEGURIDAD FÍSICA

SE DEBIERAN UTILIZAR PERÍMETROS DE SEGURIDAD TALES COMO PAREDES, REJAS DE ENTRADA CONTROLADAS POR TARJETAS O RECEPCIONISTAS, PARA PROTEGER LAS ÁREAS QUE CONTIENEN INFORMACIÓN Y MEDIOS DE PROCESAMIENTO DE INFORMACIÓN.


Physical Security
Data Center Uptime
Security Operations Center Controls



CONTROLES DE INGRESO FISICO

LAS ÁREAS SEGURAS DEBEN PROTEGERSE MEDIANTE CONTROLES DE INGRESO APROPIADOS PARA ASEGURAR QUE SÓLO SE LE PERMITA EL ACCESO AL PERSONAL AUTORIZADO.

CONSIDERAR LOS SIGUIENTES LINEAMIENTOS:

a) REGISTRAR FECHA Y HORA DE ENTRADA Y SALIDA DE LOS VISITANTES
b) EL ACCESO A ÁREAS DONDE SE PROCESA O ALMACENA INFORMACIÓN SENSIBLE SE DEBIERA CONTROLAR Y RESTRINGIR SÓLO A PERSONAS AUTORIZADAS MEDIANTE CONTROLES DE AUTENTICACIÓN
c) REQUERIR QUE LOS USUARIOS EMPLEADOS, CONTRATISTAS Y TERCERAS PERSONAS UTILICEN UNA IDENTIFICACIÓN VISIBLE.
d) AL PERSONAL DE SERVICIO DE APOYO DE TERCEROS SE LE DEBIERA OTORGAR ACCESO RESTRINGIDO A LAS ÁREAS SEGURAS O LOS MEDIOS DE PROCESAMIENTO DE INFORMACIÓN CONFIDENCIAL, SOLO CUANDO SEA NECESARIO; ESTE ACCESO DEBIERA SER AUTORIZADO Y MONITOREADO.
e) LOS DERECHOS DE ACCESO A ÁREAS SEGURAS DEBIERAN SER REVISADOS Y ACTUALIZADOS REGULARMENTE, Y REVOCADOS CUANDO SEA NECESARIO.

PROTECCIÓN CONTRA AMENAZAS INTERNAS Y EXTERNAS

ASIGNAR Y APLICAR PROTECCIÓN FÍSICA CONTRA DAÑO POR FUEGO, INUNDACIÓN, U OTRAS FORMAS DE DESASTRES NATURALES O CAUSADOS POR EL HOMBRE.

CONSIDERAR LOS SIGUIENTES LINEAMIENTOS PARA EVITAR DAÑOS:

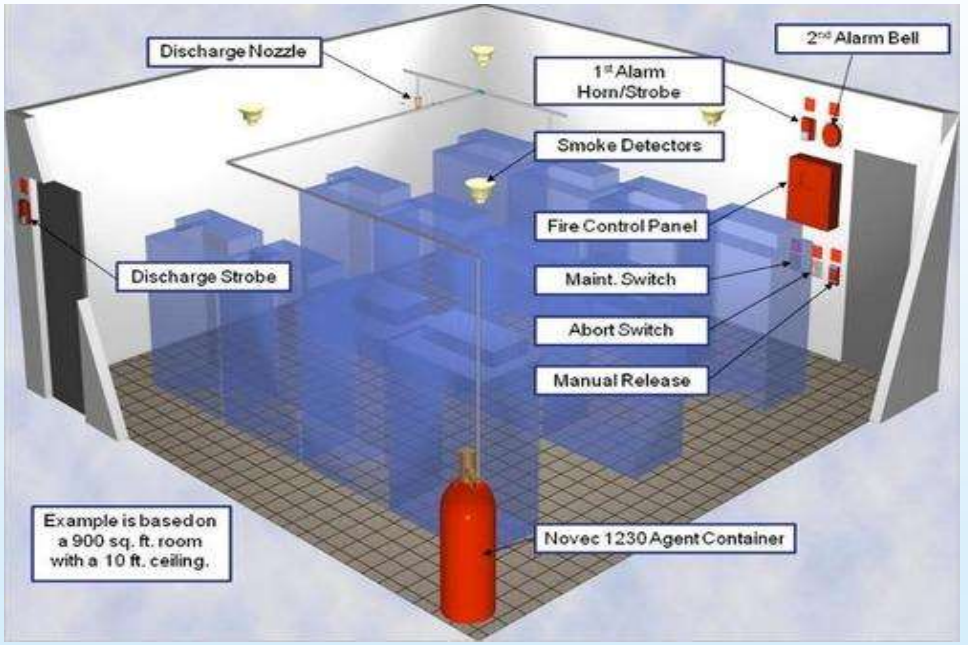
A) LOS MATERIALES PELIGROSOS O COMBUSTIBLES DEBIERAN SER ALMACENADOS A UNA DISTANCIA SEGURA DEL ÁREA ASEGURADA. LOS SUMINISTROS A GRANEL COMO PAPELERÍA NO DEBIERA ALMACENARSE EN EL ÁREA ASEGURADA.

B) EL EQUIPO DE REEMPLAZO Y LOS MEDIOS DE RESPALDO DEBIERAN UBICARSE A UNA DISTANCIA SEGURA PARA EVITAR EL DAÑO DE UN DESASTRE QUE AFECTE EL LOCAL PRINCIPAL.

C) PROPORCIONAR EQUIPO CONTRA-INCENDIOS UBICADO ADECUADAMENTE.

Fire extinguishing methods

Class	Description (Fuel)	Extinguishing Method
A	Common combustibles such as paper, wood, furniture, clothing	Water, Foam
B	Burnable fuels such as gasoline or oil	Inert Gas, CO_2
C	Electrical fires such as computers and electronics	Inert Gas, CO_2 (Note: Most important step: Turn off electricity first!)
D	Special fires, such as chemical, metal	Dry Powder (May require total immersion or other special techniques)
K	Commercial kitchen fire	Wet Chemicals



TRABAJO EN AREAS ASEGURADAS

CONSIDERAR LOS SIGUIENTES LINEAMIENTOS:

A) EL PERSONAL DEBIERA ESTAR AL TANTO DE LA EXISTENCIA O LAS ACTIVIDADES DENTRO DEL ÁREA ASEGURADA SÓLO CONFORME LAS NECESITE CONOCER.
B) SE DEBIERA EVITAR EL TRABAJO NO-SUPERVISADO EN EL ÁREA ASEGURADA TANTO POR RAZONES DE SEGURIDAD COMO PARA EVITAR LAS OPORTUNIDADES PARA ACTIVIDADES MALICIOSOS.
C) LAS ÁREAS ASEGURADAS VACÍAS DEBIERAN SER CERRADAS FÍSICAMENTE BAJO LLAVE Y REVISADAS PERIÓDICAMENTE;
D) NO SE DEBIERA PERMITIR EQUIPO FOTOGRÁFICO, DE VÍDEO, AUDIO Y OTRO EQUIPO DE GRABACIÓN.
COMO CÁMARAS EN EQUIPOS MÓVILES; A NO SER QUE SEA AUTORIZADO.

LOS ARREGLOS PARA TRABAJAR EN LAS ÁREAS ASEGURADAS INCLUYEN CONTROLES PARA LOS EMPLEADOS, CONTRATISTAS Y TERCEROS QUE TRABAJEN EN EL ÁREA ASEGURADA, ASÍ COMO OTRAS ACTIVIDADES DE TERCEROS QUE ALLÍ SE REALICEN.

UBICACIÓN Y PROTECCIÓN DEL EQUIPO

CONSIDERAR LOS SIGUIENTES LINEAMIENTOS PARA LA PROTECCIÓN DEL EQUIPO:

A) EL EQUIPO SE DEBIERA UBICAR DE MANERA QUE SE MINIMICE EL ACCESO INNECESARIO A LAS ÁREAS DE TRABAJO;
B) LOS MEDIOS DE PROCESAMIENTO DE LA INFORMACIÓN QUE MANEJAN DATA CONFIDENCIA DEBIERAN UBICARSE DE MANERA QUE SE RESTRINJA EL ÁNGULO DE VISIÓN PARA REDUCIR EL RIESGO QUE LA INFORMACIÓN SEA VISTA POR PERSONAS NO AUTORIZADAS DURANTE SU USO; Y SE DEBIERAN ASEGURAR LOS MEDIOS DE ALMACENAJE PARA EVITAR EL ACCESO NO AUTORIZADO;
C) AISLAR LOS ÍTEMS QUE REQUIEREN PROTECCIÓN ESPECIAL PARA REDUCIR EL NIVEL GENERAL DE LA PROTECCIÓN REQUERIDA;
D) ADOPTAR CONTROLES PARA MINIMIZAR EL RIESGO DE AMENAZAS POTENCIALES; POR EJEMPLO, ROBO, FUEGO, EXPLOSIVOS, HUMO, AGUA (O FALLA EN EL SUMINISTRO DE AGUA), POLVO, VIBRACIÓN, EFECTOS QUÍMICOS, INTERFERENCIAS EN EL SUMINISTRO ELÉCTRICO, INTERFERENCIA EN LAS COMUNICACIONES, RADIACIÓN ELECTROMAGNÉTICA Y VANDALISMO

UBICACIÓN Y PROTECCIÓN DEL EQUIPO

CONSIDERAR LOS SIGUIENTES LINEAMIENTOS PARA LA PROTECCIÓN DEL EQUIPO:

E) ESTABLECER LINEAMIENTOS SOBRE COMER, BEBER Y FUMAR EN LA PROXIMIDAD DE LOS MEDIOS DE PROCESAMIENTO DE INFORMACIÓN.
F) MONITOREAR LAS CONDICIONES AMBIENTALES TALES COMO TEMPERATURA Y HUMEDAD, QUE PUDIERA AFECTAR ADVERSAMENTE LA OPERACIÓN DE LOS MEDIOS DE PROCESAMIENTO DE LA INFORMACIÓN.

PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS

LOS PROCEDIMIENTOS DE OPERACIÓN SE DEBIERAN DOCUMENTAR, MANTENER Y PONER A DISPOSICIÓN DE TODOS LOS USUARIOS QUE LOS NECESITEN.
SE DEBIERAN PREPARAR PROCEDIMIENTOS DOCUMENTADOS PARA LAS ACTIVIDADES DEL SISTEMA ASOCIADAS CON LOS MEDIOS DE PROCESAMIENTO DE LA INFORMACIÓN Y COMUNICACIÓN; TALES COMO PROCEDIMIENTOS PARA ENCENDER Y APAGAR COMPUTADORAS, COPIAS DE SEGURIDAD, MANTENIMIENTO DEL EQUIPO, MANEJO DE MEDIOS, CUARTO DE CÓMPUTO, MANEJO DEL CORREO Y SEGURIDAD.

LOS PROCEDIMIENTOS DE OPERACIÓN DEBIERAN ESPECIFICAR LAS INSTRUCCIONES PARA LA EJECUCIÓN DETALLADA DE CADA TRABAJO INCLUYENDO:

A) PROCESAMIENTO Y MANEJO DE INFORMACIÓN;
B) COPIA DE SEGURIDAD O RESPALDO
C) REQUERIMIENTOS DE PROGRAMACIÓN DE HORARIOS, INCLUYENDO LAS INTERDEPENDENCIAS CON OTROS SISTEMAS, LOS TIEMPOS DE CULMINACIÓN Y HORARIOS DE LOS PRIMEROS Y ÚLTIMOS TRABAJOS;
D) INSTRUCCIONES PARA EL MANEJO DE ERRORES U OTRAS CONDICIONES EXCEPCIONALES, LAS CUALES PODRÍAN SURGIR DURANTE LA EJECUCIÓN DEL TRABAJO, INCLUYENDO LAS RESTRICCIONES SOBRE EL USO DE LAS UTILIDADES DEL SISTEMA
E) CONTACTOS DE SOPORTE EN EL EVENTO DE DIFICULTADES OPERACIONALES O TÉCNICAS INESPERADAS;
F) INSTRUCCIONES PARA EL MANEJO DE OUTPUT ESPECIAL Y MEDIOS, TALES COMO EL USO DE PAPELERÍA ESPECIAL O EL MANEJO DE OUTPUT CONFIDENCIAL INCLUYENDO LOS PROCEDIMIENTOS PARA LA ELIMINACIÓN SEGURA DEL OUTPUT DE TRABAJO FALLIDOS
G) PROCEDIMIENTOS DE REINICIO Y RECUPERACIÓN DEL SISTEMA PARA SU USO EN EL EVENTO DE UNA FALLA EN EL SISTEMA;
H) LA GESTIÓN DE LA INFORMACIÓN DEL RASTRO DE AUDITORÍA Y REGISTRO DEL SISTEMA.

RESPALDO O BACKUP

OBJETIVO: MANTENER LA INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN Y LOS MEDIOS DE PROCESAMIENTO DE INFORMACIÓN.
SE DEBIERAN ESTABLECER LOS PROCEDIMIENTOS DE RUTINA PARA IMPLEMENTAR LA POLÍTICA DE RESPALDO ACORDADA Y LA ESTRATEGIA PARA TOMAR COPIAS DE RESPALDO DE LA DATA Y PRACTICAR SU RESTAURACIÓN OPORTUNA.

SE DEBIERAN HACER COPIAS DE RESPALDO DE LA INFORMACIÓN Y SOFTWARE Y SE DEBIERAN PROBAR REGULARMENTE EN CONCORDANCIA CON LA POLÍTICA DE COPIAS DE RESPALDO ACORDADA.
LINEAMIENTO DE IMPLEMENTACIÓN SE DEBIERA PROPORCIONAR MEDIOS DE RESPALDO ADECUADOS PARA ASEGURAR QUE TODA LA INFORMACIÓN ESENCIAL Y SOFTWARE SE PUEDA RECUPERAR DESPUÉS DE UN DESASTRE O FALLA DE MEDIOS:
SE DEBIERAN CONSIDERAR LOS SIGUIENTES ÍTEMS PARA EL RESPALDO DE LA INFORMACIÓN:

A) SE DEBIERA DEFINIR EL NIVEL NECESARIO DE RESPALDO DE LA INFORMACIÓN;
B) SE DEBIERAN PRODUCIR REGISTROS EXACTOS Y COMPLETOS DE LAS COPIAS DE RESPALDO Y PROCEDIMIENTOS DOCUMENTADOS DE LA RESTAURACIÓN;
C) LA EXTENSIÓN (POR EJEMPLO, RESPALDO COMPLETO O DIFERENCIAL) Y LA FRECUENCIA DE LOS RESPALDOS DEBIERA REFLEJAR LOS REQUERIMIENTOS COMERCIALES DE LA ORGANIZACIÓN, LOS REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN INVOLUCRADA, Y EL GRADO CRÍTICO DE LA INFORMACIÓN PARA LA OPERACIÓN CONTINUA DE LA ORGANIZACIÓN;
D) LAS COPIAS DE RESPALDO SE DEBIERAN ALMACENAR EN UN LUGAR APARTADO, A LA DISTANCIA SUFICIENTE COMO PARA ESCAPAR DE CUALQUIER DAÑO POR UN DESASTRE EN EL LOCAL PRINCIPAL

E) A LA INFORMACIÓN DE RESPALDO SE LE DEBIERA DAR EL NIVEL DE PROTECCIÓN FÍSICA Y AMBIENTAL APROPIADO CONSISTENTE CON LOS ESTÁNDARES APLICADOS EN EL LOCAL PRINCIPAL; LOS CONTROLES APLICADOS A LOS MEDIOS EN EL LOCAL PRINCIPAL SE DEBIERA EXTENDER PARA CUBRIR LA UBICACIÓN DE LA COPIA DE RESPALDO;
F) LOS MEDIOS DE RESPALDO SE DEBIERAN PROBAR REGULARMENTE PARA ASEGURAR QUE SE PUEDAN CONFIAR EN ELLOS PARA USARLOS CUANDO SEA NECESARIA EN CASO DE EMERGENCIA;
G) LOS PROCEDIMIENTOS DE RESTAURACIÓN SE DEBIERAN CHEQUEAR Y PROBAR REGULARMENTE PARA ASEGURAR QUE SEAN EFECTIVOS Y QUE PUEDEN SER COMPLETADOS DENTRO DEL TIEMPO ASIGNADO EN LOS PROCEDIMIENTOS OPERACIONALES PARA LA RECUPERACIÓN;
H) EN SITUACIONES CUANDO LA CONFIDENCIALIDAD ES DE IMPORTANCIA, LAS COPIAS DE RESPALDO DEBIERAN SER PROTEGIDAS POR MEDIOS DE UNA CODIFICACIÓN.

LOS PROCEDIMIENTOS DE RESPALDO PARA LOS SISTEMAS INDIVIDUALES DEBIERAN SER PROBADOS REGULARMENTE PARA ASEGURAR QUE CUMPLAN CON LOS REQUERIMIENTOS DE LOS PLANES DE CONTINUIDAD DEL NEGOCIO. PARA SISTEMAS CRÍTICOS, LOS PROCEDIMIENTOS DE RESPALDO DEBIERAN ABARCAR TODA LA INFORMACIÓN, APLICACIONES Y DATA DE TODOS LOS SISTEMAS, NECESARIOS PARA RECUPERAR EL SISTEMA COMPLETO EN CASO DE UN DESASTRE.

SE DEBIERA DETERMINAR EL PERÍODO DE RETENCIÓN PARA LA INFORMACIÓN COMERCIAL ESENCIAL, Y TAMBIÉN CUALQUIER REQUERIMIENTO PARA QUE LAS COPIAS DE ARCHIVO SE MANTENGAN PERMANENTEMENTE.
LOS PROCEDIMIENTOS DE RESPALDO PUEDEN SER AUTOMATIZADOS PARA FACILITAR EL PROCESO DE RESPALDO Y RESTAURACIÓN. ESTAS SOLUCIONES AUTOMATIZADAS DEBIERAN SER PROBADAS SUFICIENTEMENTE ANTES DE SU IMPLEMENTACIÓN Y TAMBIÉN A INTERVALOS REGULARES.

CONTROLES DE REDES

LAS REDES DEBIERAN SER ADECUADAMENTE MANEJADAS Y CONTROLADAS PARA PODER PROTEGER LA INFORMACIÓN EN LAS REDES, Y MANTENER LA SEGURIDAD DE LOS SISTEMAS Y APLICACIONES UTILIZANDO LA RED, INCLUYENDO LA INFORMACIÓN EN TRÁNSITO.

LOS ADMINISTRADORES DE LA RED DEBIERAN IMPLEMENTAR CONTROLES PARA ASEGURAR LA SEGURIDAD DE LA INFORMACIÓN EN LAS REDES, Y PROTEGER LOS SERVICIOS CONECTADOS DE ACCESOS NO-AUTORIZADOS. EN PARTICULAR, SE DEBIERAN CONSIDERAR LOS SIGUIENTES ÍTEMS:

A) CUANDO SEA APROPIADO, LA RESPONSABILIDAD OPERACIONAL PARA LAS REDES SE DEBIERA SEPARAR DE LAS OPERACIONES DE CÓMPUTO (RED DE ADMINISTRACIÓN O MANAGEMENT);
B) SE DEBIERAN ESTABLECER LAS RESPONSABILIDADES Y PROCEDIMIENTOS PARA LA GESTIÓN DEL EQUIPO REMOTO, INCLUYENDO EL EQUIPO EN LAS ÁREAS DEL USUARIO;
C) SE DEBIERAN ESTABLECER CONTROLES ESPECIALES PARA SALVAGUARDAR LA CONFIDENCIALIDAD Y LA INTEGRIDAD DE LA DATA QUE PASA A TRAVÉS DE LAS REDES PÚBLICAS O A TRAVÉS DE LAS REDES INALÁMBRICAS; Y PROYECTAR LOS SISTEMAS Y APLICACIONES CONECTADOS.
TAMBIÉN SE PUEDEN REQUERIR CONTROLES ESPECIALES PARA MANTENER LA DISPONIBILIDAD DE LOS SERVICIOS DE LA RED Y LAS COMPUTADORAS CONECTADAS;
D) SE DEBIERA APLICAR REGISTROS DE INGRESO Y MONITOREO APROPIADOS PARA PERMITIR EL REGISTRO DE LAS ACCIONES DE SEGURIDAD RELEVANTES;
E) LAS ACTIVIDADES DE GESTIÓN DEBIERAN ESTAR ESTRECHAMENTE COORDINADAS PARA OPTIMIZAR EL SERVICIO A LA ORGANIZACIÓN Y PARA ASEGURAR QUE LOS CONTROLES SEAN APLICADOS CONSISTENTEMENTE A TRAVÉS DE LA INFRAESTRUCTURA DE PROCESAMIENTO DE LA INFORMACIÓN.

SEGREGACIÓN DE REDES

LOS GRUPOS DE SERVICIOS DE INFORMACIÓN, USUARIOS Y SISTEMAS DE INFORMACIÓN DEBIERAN SER SEGREGADOS EN REDES.

UN MÉTODO PARA CONTROLAR LA SEGURIDAD DE GRANDES REDES ES DIVIDIRLAS EN DOMINIOS DE RED LÓGICOS SEPARADOS; POR EJEMPLO, DOMINIOS DE RED INTERNOS Y DOMINIOS DE RED EXTERNOS DE UNA ORGANIZACIÓN; CADA UNO PROTEGIDO POR UN PERÍMETRO DE SEGURIDAD DEFINIDO. SE PUEDE APLICAR UN CONJUNTO DE CONTROLES GRADUADOS EN DOMINIOS DE RED LÓGICOS DIFERENTES PARA SEGREGAR AÚN MÁS
LOS AMBIENTES DE SEGURIDAD DE LA RED; POR EJEMPLO, SISTEMAS DE ACCESO PÚBLICO, REDES INTERNAS Y ACTIVOS CRÍTICOS.
LOS DOMINIOS DEBIERAN SER DEFINIDOS EN BASE A UNA EVALUACIÓN DEL RIESGO Y LOS REQUERIMIENTOS DE SEGURIDAD DIFERENTES DENTRO DE CADA UNO DE LOS DOMINIOS.
ESTE TIPO DE PERÍMETRO DE RED SE PUEDE IMPLEMENTAR INSTALANDO UN GATEWAY SEGURO ENTRE DOS REDES PARA MANTENERLAS INTERCONECTADAS Y CONTROLAR EL ACCESO Y EL FLUJO DE INFORMACIÓN ENTRE LOS DOS DOMINIOS. ESTE GATEWAY DEBIERA ESTAR CONFIGURADO PARA FILTRAR EL TRÁFICO ENTRE ESTOS DOMINIOS Y PARA BLOQUEAR EL ACCESO NO-AUTORIZADO EN CONCORDANCIA CON LA POLÍTICA DE CONTROL DE ACCESO DE LA ORGANIZACIÓN. UN EJEMPLO DE ESTE TIPO DE GATEWAY ES LO QUE COMÚNMENTE SE CONOCE COMO UN FIREWALL. OTRO MÉTODO PARA SEGREGAR DOMINIOS LÓGICOS SEPARADOS ES RESTRINGIR EL ACCESO A LA RED UTILIZANDO REDES PRIVADAS VIRTUALES PARA GRUPOS DE USUARIOS DENTRO DE LA ORGANIZACIÓN.

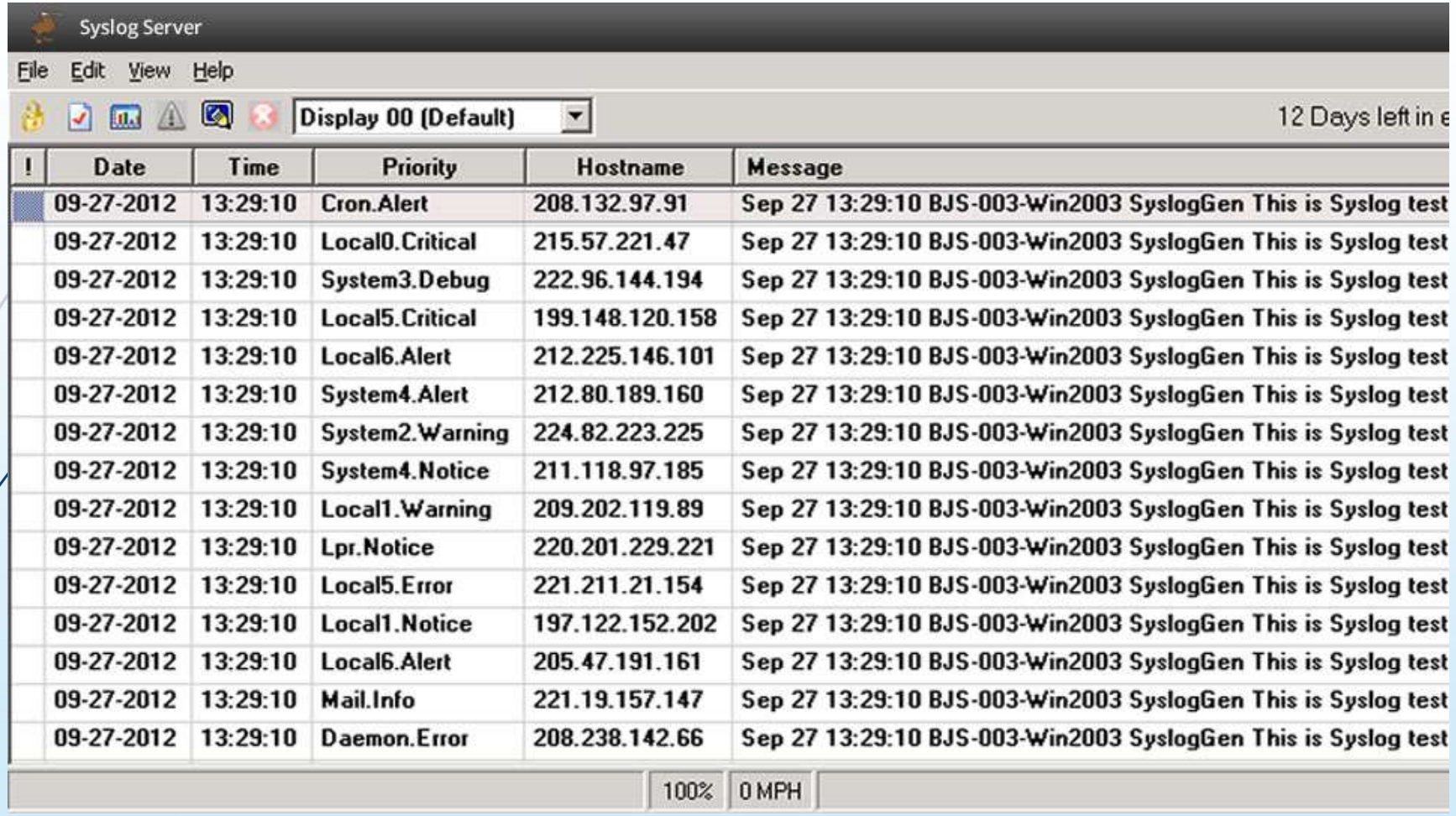
MONITOREO

DETECTAR LAS ACTIVIDADES DE PROCESAMIENTO DE INFORMACIÓN NO AUTORIZADAS.

SE DEBIERAN MONITOREAR LOS SISTEMAS Y SE DEBIERAN REPORTAR LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN. SE DEBIERAN UTILIZAR BITÁCORAS DE OPERADOR Y SE DEBIERAN REGISTRAR LAS FALLAS PARA ASEGURAR QUE SE IDENTIFIQUEN LOS PROBLEMAS EN LOS SISTEMAS DE INFORMACIÓN.

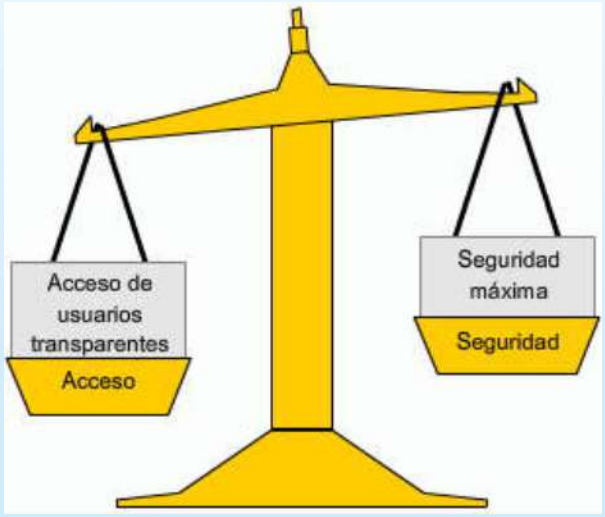
UNA ORGANIZACIÓN DEBIERA CUMPLIR CON TODOS LOS REQUERIMIENTOS LEGALES RELEVANTES APLICABLES A SUS ACTIVIDADES DE MONITOREO Y REGISTRO.

SE DEBIERA UTILIZAR EL MONITOREO DEL SISTEMA PARA CHEQUEAR LA EFECTIVIDAD DE LOS CONTROLES ADOPTADOS Y PARA VERIFICAR LA CONFORMIDAD CON UN MODELO DE POLÍTICA DE ACCESO.


Syslog Server
File Edit View Help
Display 00 (Default)
12 Days left in e
! Date Time Priority Hostname Message
09-27-2012 13:29:10 Cron.Alert 208.132.97.91 Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test
09-27-2012 13:29:10 Local0.Critical 215.57.221.47 Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test
09-27-2012 13:29:10 System3.Debug 222.96.144.194 Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test
09-27-2012 13:29:10 Local5.Critical 199.148.120.158 Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test
09-27-2012 13:29:10 Local6.Alert 212.225.146.101 Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test
09-27-2012 13:29:10 System4.Alert 212.80.189.160 Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test
09-27-2012 13:29:10 System2.Warning 224.82.223.225 Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test
09-27-2012 13:29:10 System4.Notice 211.118.97.185 Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test
09-27-2012 13:29:10 Local1.Warning 209.202.119.89 Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test
09-27-2012 13:29:10 Lpr.Notice 220.201.229.221 Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test
09-27-2012 13:29:10 Local5.Error 221.211.21.154 Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test
09-27-2012 13:29:10 Local1.Notice 197.122.152.202 Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test
09-27-2012 13:29:10 Local6.Alert 205.47.191.161 Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test
09-27-2012 13:29:10 Mail.Info 221.19.157.147 Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test
09-27-2012 13:29:10 Daemon.Error 208.238.142.66 Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test
100%
0 MPH

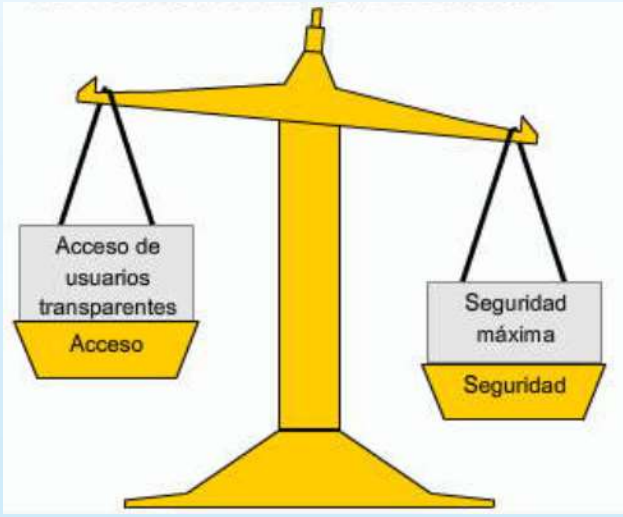
REDES ABIERTAS

- Fácil configuración
- Bajo costo de administración



REDES CERRADAS

- Configuración compleja
- Mayor costo de administración



RELEVAMIENTO DEL TRÁFICO EN EL DATACENTER

SE DEBERÁ TENER CONOCIMIENTO DEL TRÁFICO EXISTENTE, EL TRÁFICO INVOLUCRADO EN TAREAS ESPECÍFICAS Y EL TRÁFICO PARÁSITO O INNECESARIO, EL CUAL DEBERÍA SER ELIMINADO O AISLADO.

PARA REALIZAR DICHO RELEVAMIENTO, SERÁ NECESARIA LA UTILIZACIÓN DE UTILITARIOS, SNIFFERS U OTRAS HERRAMIENTAS QUE REVELEN EL FLUJO DE TRÁFICO EXISTENTE.

LA ELIMINACIÓN O STOP DE SERVICIOS INNECESARIOS MEJORA TANTO LA SEGURIDAD (EVITANDO POTENCIALES VULNERABILIDADES), COMO LA PERFORMANCE (EVITANTO EL FORWARDING DE TRÁFICO SIN UTILIDAD).

EN UN ENTORNO NORMAL, PODRÍAMOS TENER EN CUENTA LOS SIGUIEMTES SERVICIOS:

TRÁFICO DE PRODUCCIÓN:

HTTP, SQL, LDAP, DNS, SMTP, POP3, NFS, SAP, AS/400 (SNA)

TRÁFICO DE GESTIÓN

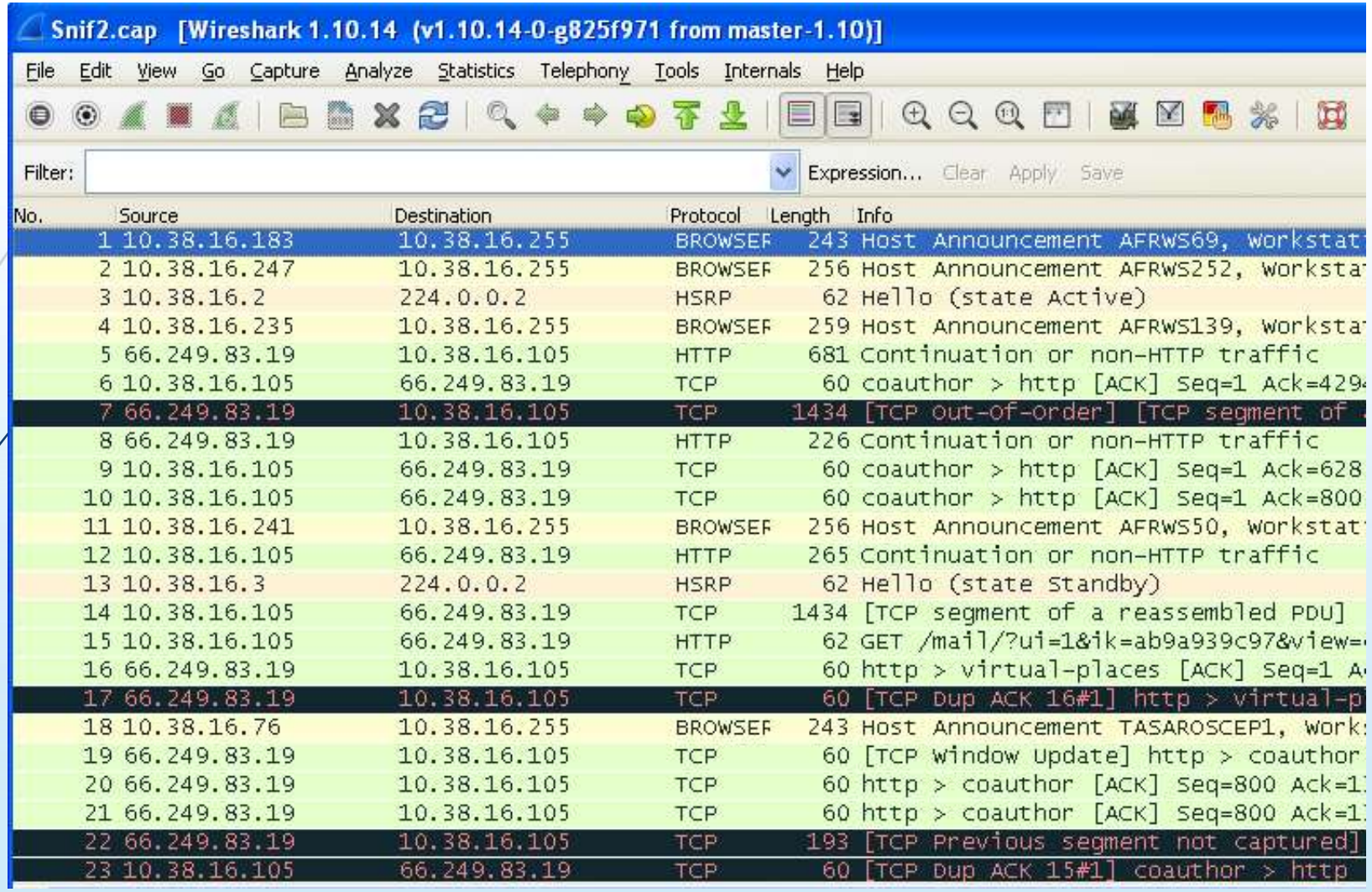
SYSLOG, SNMP, SSH, TELNET, NTP, NETFLOW, RDP, CONTROL REMOTO, RADIUS, TACACS+,

TRÁFICO OPERATIVO DE LA RED:

ARP, DHCP, ICMP, VTP, DTP, STP, CDP, OSPF, EIGRP

TRÁFICO DE VOIP:

H.323, SIP, SCCP, RTP, SRTP


Snif2.cap [Wireshark 1.10.14 (v1.10.14-0-g825f971 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Source Destination Protocol Length Info
1 10.38.16.183 10.38.16.255 BROWSER 243 Host Announcement AFRWS69, Workstat
2 10.38.16.247 10.38.16.255 BROWSER 256 Host Announcement AFRWS252, Workstat
3 10.38.16.2 224.0.0.2 HSRP 62 Hello (state Active)
4 10.38.16.235 10.38.16.255 BROWSER 259 Host Announcement AFRWS139, Workstat
5 66.249.83.19 10.38.16.105 HTTP 681 Continuation or non-HTTP traffic
6 10.38.16.105 66.249.83.19 TCP 60 coauthor > http [ACK] Seq=1 Ack=429
7 66.249.83.19 10.38.16.105 TCP 1434 [TCP Out-Of-Order] [TCP segment of
8 66.249.83.19 10.38.16.105 HTTP 226 Continuation or non-HTTP traffic
9 10.38.16.105 66.249.83.19 TCP 60 coauthor > http [ACK] Seq=1 Ack=628
10 10.38.16.105 66.249.83.19 TCP 60 coauthor > http [ACK] Seq=1 Ack=800
11 10.38.16.241 10.38.16.255 BROWSER 256 Host Announcement AFRWS50, Workstat
12 10.38.16.105 66.249.83.19 HTTP 265 Continuation or non-HTTP traffic
13 10.38.16.3 224.0.0.2 HSRP 62 Hello (state Standby)
14 10.38.16.105 66.249.83.19 TCP 1434 [TCP segment of a reassembled PDU]
15 10.38.16.105 66.249.83.19 HTTP 62 GET /mail/?ui=1&ik=ab9a939c97&view=
16 66.249.83.19 10.38.16.105 TCP 60 http > virtual-places [ACK] Seq=1 A
17 66.249.83.19 10.38.16.105 TCP 60 [TCP Dup ACK 16#1] http > virtual-p
18 10.38.16.76 10.38.16.255 BROWSER 243 Host Announcement TASAROSCEP1, Work
19 66.249.83.19 10.38.16.105 TCP 60 [TCP Window Update] http > coauthor
20 66.249.83.19 10.38.16.105 TCP 60 http > coauthor [ACK] Seq=800 Ack=1
21 66.249.83.19 10.38.16.105 TCP 60 http > coauthor [ACK] Seq=800 Ack=1
22 66.249.83.19 10.38.16.105 TCP 193 [TCP Previous segment not captured]
23 10.38.16.105 66.249.83.19 TCP 60 [TCP Dup ACK 15#1] coauthor > http

MANTENIMIENTO Y MONITOREO DEL DATACENTER

Los datacenters están dotados de equipos eléctricos e informáticos que deben funcionar siempre. Esto quiere decir que, para evitar su deterioro, TODO lo que esté en la infraestructura debe recibir revisiones, verificaciones y mantenimiento. Pueden parecer procesos tediosos, pero son pequeños pasos que sirven para evitar problemas mayores

- MANTENIMIENTO DE RED
- CLIMATIZACIÓN
- CONTROL DE INCENDIOS
- CONTROL DE ACCESO
- GRUPO ELECTRÓGENO
- SISTEMA DE ALIMENTACIÓN INTERRUMPIDA (UPS)

TIPOS DE MANTENIMIENTO

EXISTEN DIVERSOS TIPOS DE MANTENIMIENTO SEGÚN EL MOMENTO EN EL QUE DECIDA APLICARSE: ANTES, DURANTE O DESPUÉS DE UN FALLO.

- MANTENIMIENTO PREVENTIVO
- MANTENIMIENTO PREDICTIVO
- MANTENIMIENTO CORRECTIVO

MANTENIMIENTO PREVENTIVO

PROCEDIMIENTOS QUE BUSCAN ALARGAR LA VIDA UTIL DE LOS EQUIPOS Y REDUCIR POSIBLES FALLAS.

IMPLICA INSPECCIONES Y DETECCIÓN ANTICIPADA DE POSIBLES PROBLEMAS, REEMPLAZANDO PIEZAS, AJUSTANDO COMPONENTES Y LIMPIANDO FILTROS DE AIRE PERIODICAMENTE.

MANTENIMIENTO PREDICTIVO

SE REALIZA EN LOS EQUIPOS EN LOS QUE PUEDE PREDECIRSE QUE TENDRÁ UN FALLO INMINENTE.

GENERALMENTE EN EL DATASHEET DE CADA EQUIPO SUELE HABER UN PARAMETRO “MTBF” (tiempo medio entre fallas) QUE DA UN INDICIO DEL REEMPLAZO ANTES DE QUE COLAPSE EL DISPOSITIVO.

MANTENIMIENTO CORRECTIVO

SE REALIZA UNA VEZ QUE YA SE PRODUJO EL FALLO.

TIPOS DE MANTENIMIENTO CORRECTIVO:

- MANTENIMIENTO CORRECTIVO PROGRAMADO
- MANTENIMIENTO CORRECTIVO NO PROGRAMADO

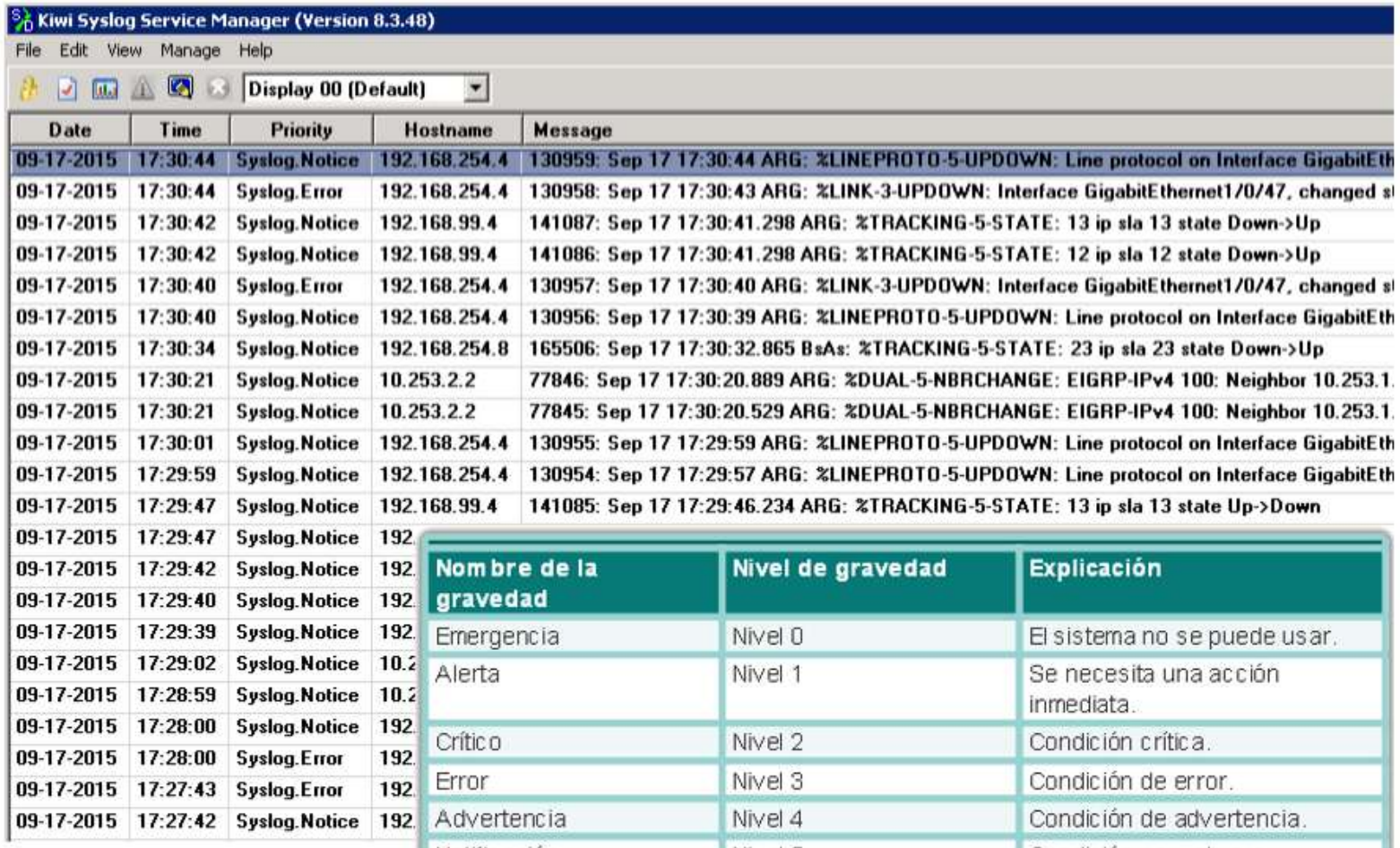
HERRAMIENTAS DE OPERACIÓN Y MANTENIMIENTO

SYSLOG

AL OCURRIR CIERTOS EVENTOS EN UNA RED LOS DISPOSITIVOS TIENEN MECANISMOS PARA NOTIFICAR MENSAJES DETALLADOS AL ADMINISTRADOR, QUE PUEDEN O NO SER IMPORTANTES.

LOS ADMINISTRADORES TIENEN VARIEDAD DE OPCIONES PARA RECIBIR, ALMACENAR E INTERPRETAR ESTOS MENSAJES.

EL MÉTODO MAS COMÚN PARA ACCEDER A LOS MENSAJES ES UTILIZANDO UN PROTOCOLO DENOMINADO "SYSLOG"



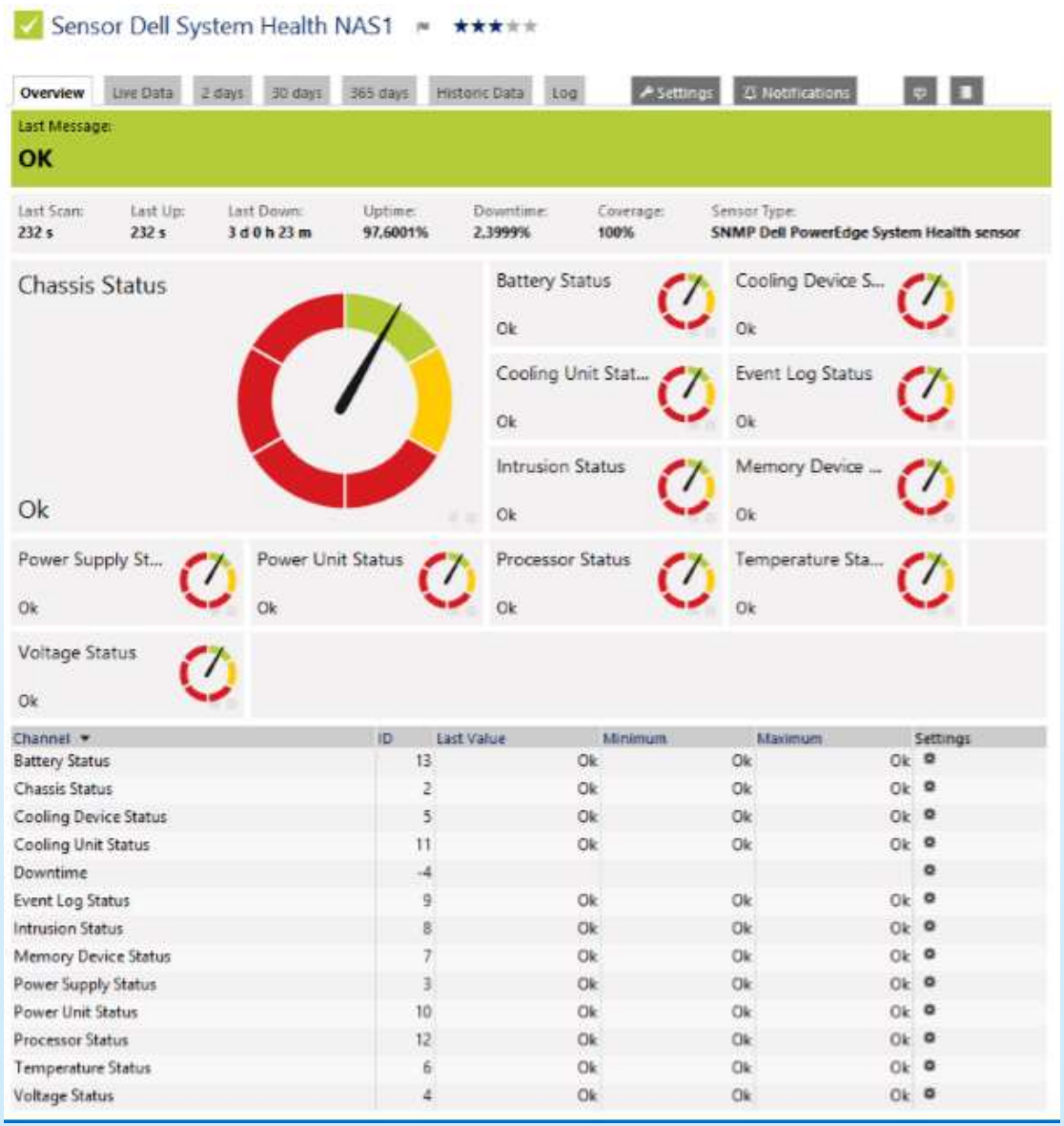
Nombre de la gravedad	Nivel de gravedad	Explicación
Emergencia	Nivel 0	El sistema no se puede usar.
Alerta	Nivel 1	Se necesita una acción inmediata.
Crítico	Nivel 2	Condición crítica.
Error	Nivel 3	Condición de error.
Advertencia	Nivel 4	Condición de advertencia.
Notificación	Nivel 5	Condición normal pero importante.
informativo	Nivel 6	Mensaje informativo.
Depuración	Nivel 7	Mensaje de depuración.

SNMP

PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE RED (SNMP)

DESARROLLADO PARA ADMINISTRAR LOS NODOS, SERVIDORES, ROUTERS Y SWITCH EN UNA RED IP.

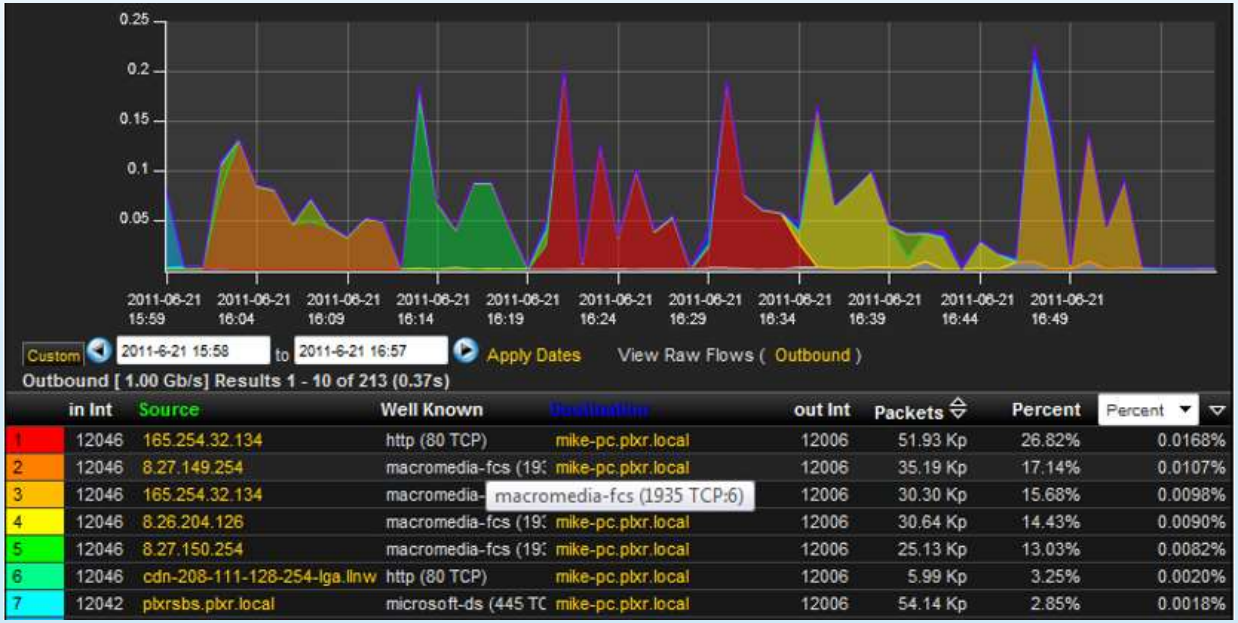
ES UN PROTOCOLO DE CAPA DE APLICACIÓN QUE PROPORCIONA UN FORMATO DE MENSAJE PARA LA COMUNICACIÓN ENTRE ADMINISTRADORES Y AGENTES.


Sensor Dell System Health NAS1
Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings
Notifications
Last Message:
OK
Last Scan: 232 s
Last Up: 232 s
Last Down: 3 d 0 h 23 m
Uptime: 97,6001%
Downtime: 2,3999%
Coverage: 100%
Sensor Type: SNMP Dell PowerEdge System Health sensor
Chassis Status
Ok
Battery Status
Ok
Cooling Device S...
Ok
Cooling Unit Stat...
Ok
Event Log Status
Ok
Intrusion Status
Ok
Memory Device ...
Ok
Power Supply St...
Ok
Power Unit Status
Ok
Processor Status
Ok
Temperature Sta...
Ok
Voltage Status
Ok
Channel
ID
Last Value
Minimum
Maximum
Settings
Battery Status 13 Ok Ok Ok
Chassis Status 2 Ok Ok Ok
Cooling Device Status 5 Ok Ok Ok
Cooling Unit Status 11 Ok Ok Ok
Downtime -4
Event Log Status 9 Ok Ok Ok
Intrusion Status 8 Ok Ok Ok
Memory Device Status 7 Ok Ok Ok
Power Supply Status 3 Ok Ok Ok
Power Unit Status 10 Ok Ok Ok
Processor Status 12 Ok Ok Ok
Temperature Status 6 Ok Ok Ok
Voltage Status 4 Ok Ok Ok

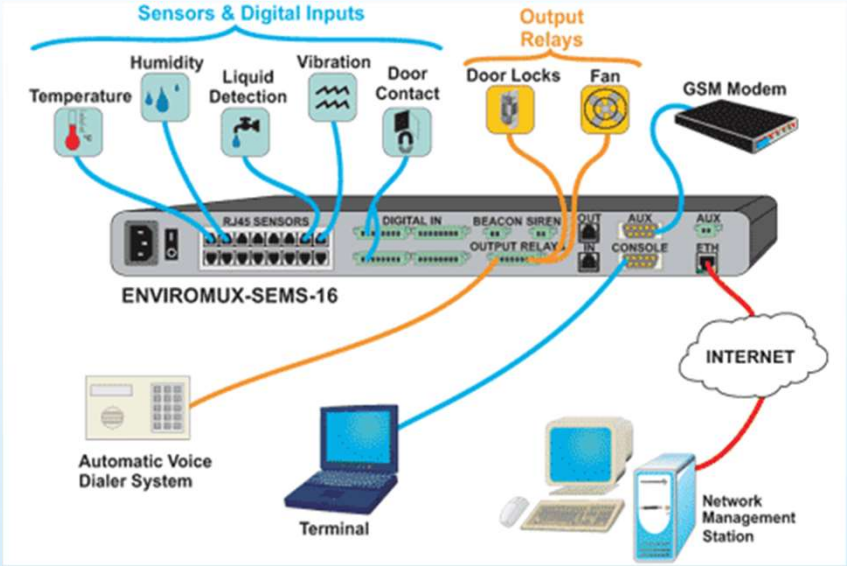
NETFLOW

ES UNA TECNOLOGÍA DE CISCO QUE PROPORCIONA ESTADÍSTICAS SOBRE LOS PAQUETES QUE FLUYEN A TRAVÉS DE UN SWITCH MULTICAPA O UN ROUTER.

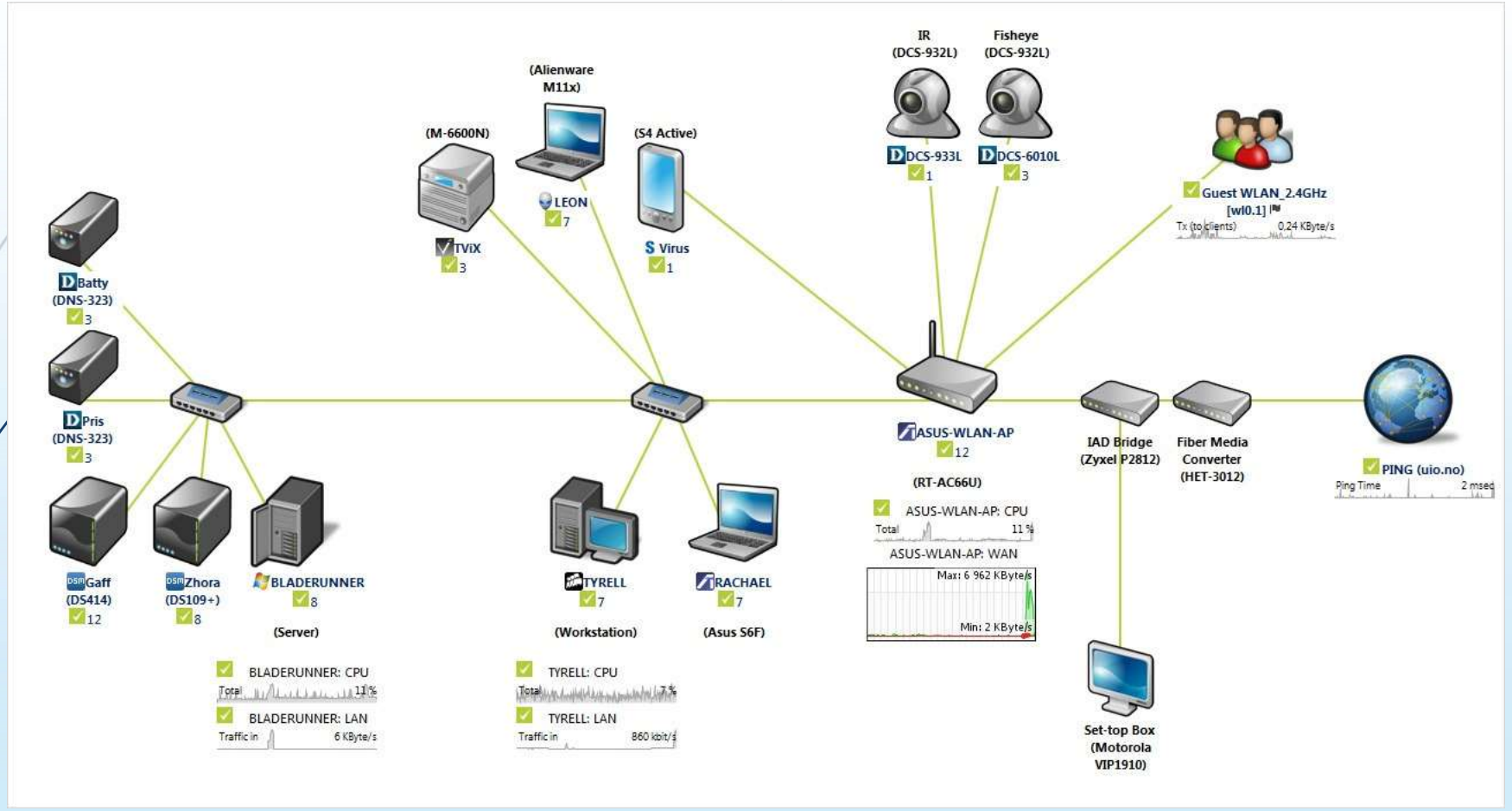
ES CASI UN ESTANDAR PARA RECOPILAR DATOS OPERATIVOS EN REDES IP



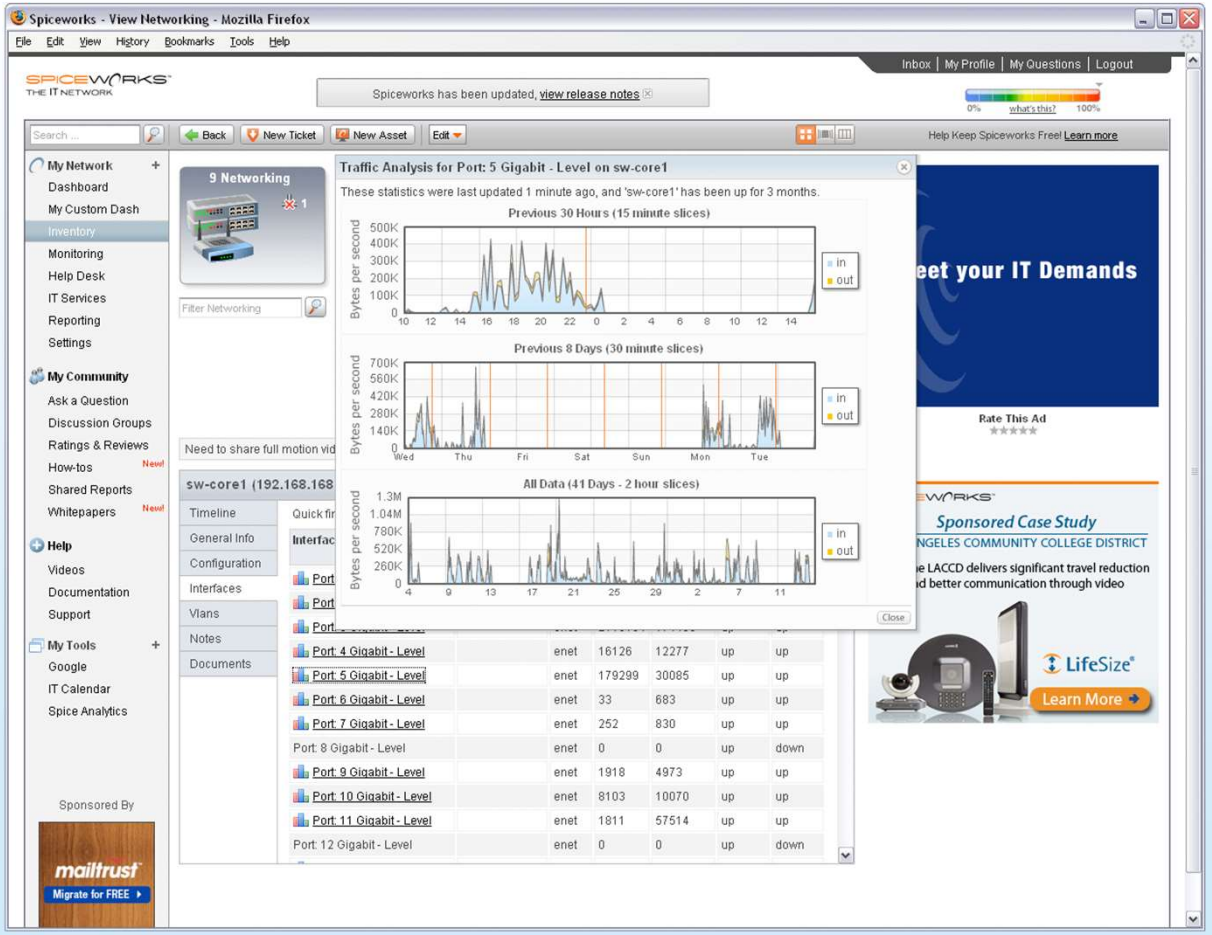
HERRAMIENTAS DE MONITOREO



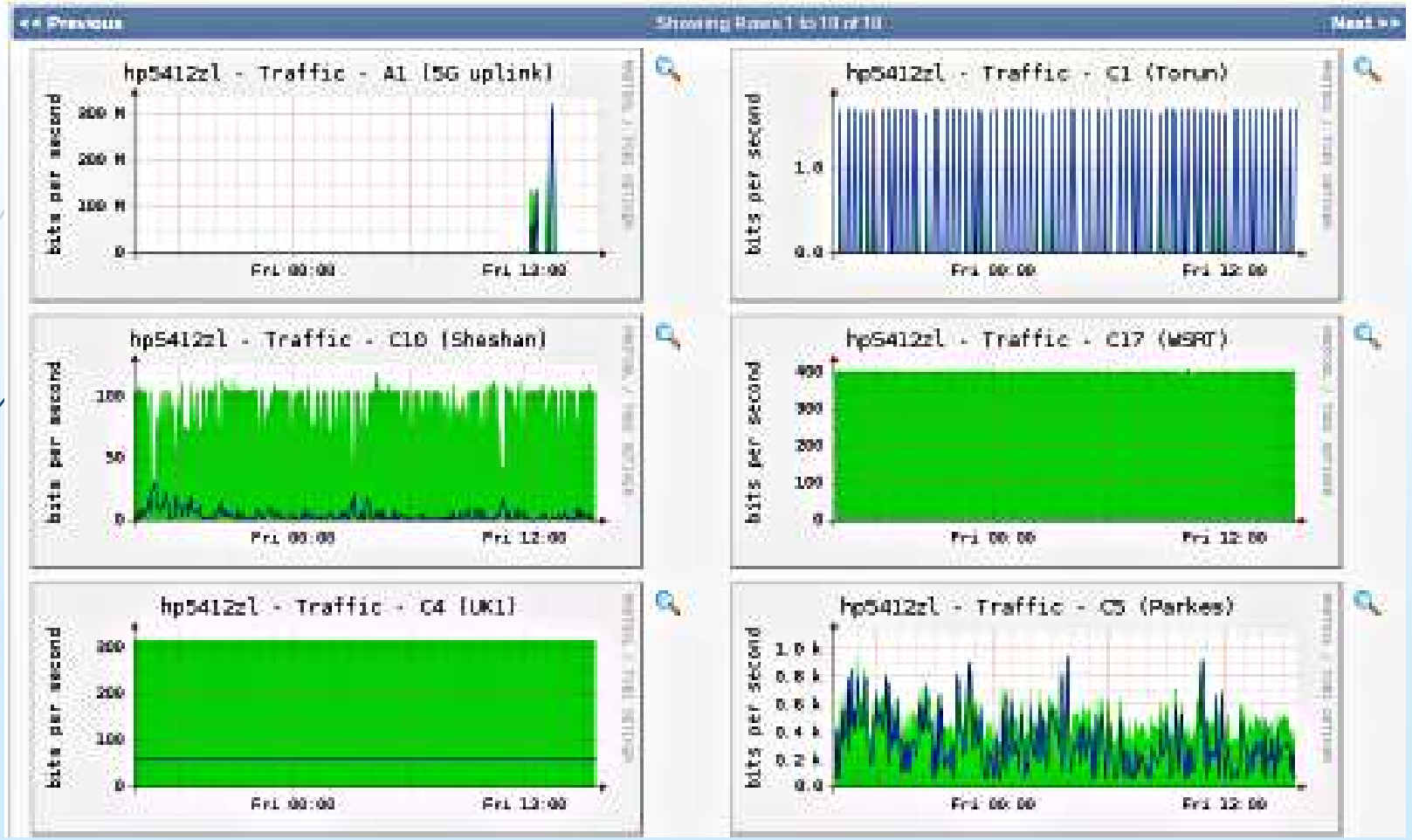
PRTG


IR
(DCS-932L)
Fisheye
(DCS-932L)
(Alienware
M11x)
(M-6600N)
(S4 Active)
DCS-933L
1
DCS-6010L
3
Guest WLAN_2.4GHz
[wl0.1]
Tx (to clients)
0.24 KByte/s
LEON
7
TViX
3
S Virus
1
Batty
(DNS-323)
3
Pris
(DNS-323)
3
ASUS-WLAN-AP
12
(RT-AC66U)
ASUS-WLAN-AP: CPU
Total
11 %
ASUS-WLAN-AP: WAN
Max: 6 962 KByte/s
Min: 2 KByte/s
IAD Bridge
(Zyxel P2812)
Fiber Media
Converter
(HET-3012)
PING (uio.no)
Ping Time
2 msec
Gaff
(DS414)
12
Zhora
(DS109+)
8
BLADERUNNER
8
(Server)
BLADERUNNER: CPU
Total
11 %
BLADERUNNER: LAN
Traffic in
6 KByte/s
TYRELL
7
(Workstation)
TYRELL: CPU
Total
7 %
TYRELL: LAN
Traffic in
860 kbit/s
RACHAEL
7
(Asus S6F)
Set-top Box
(Motorola
VIP1910)

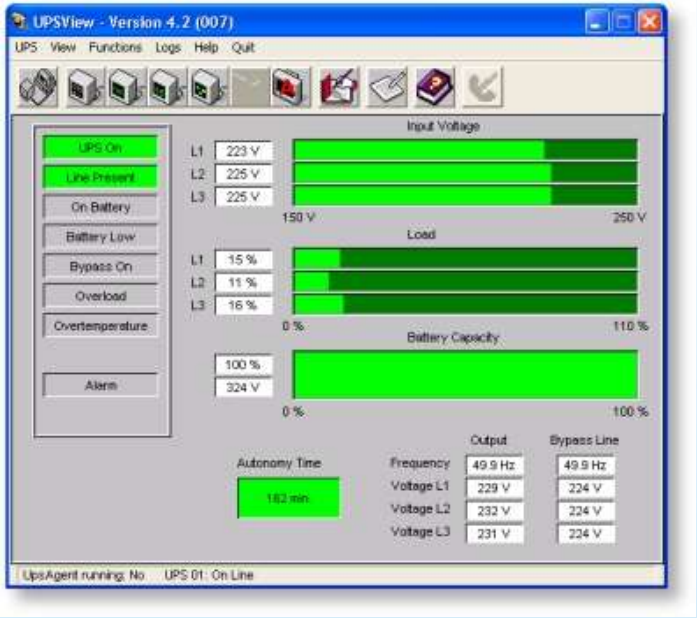
SPICEWORKS

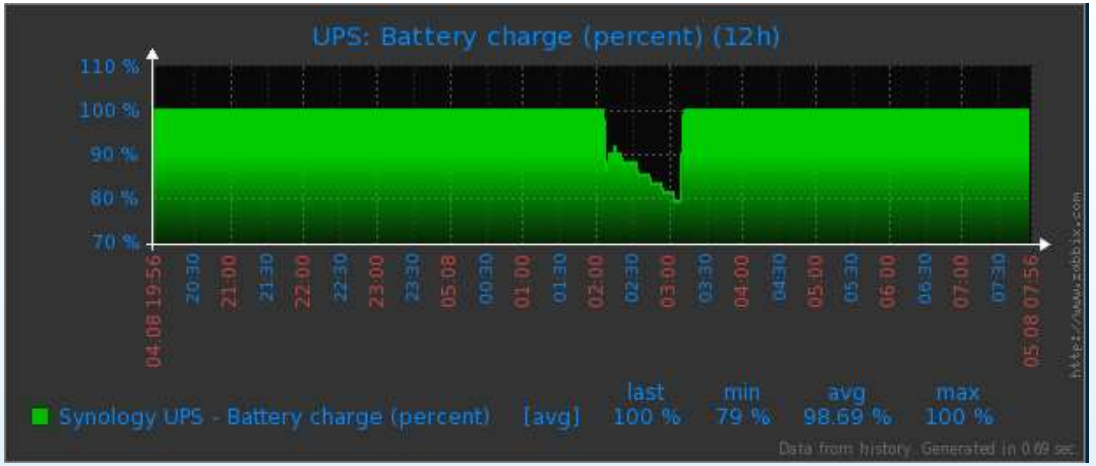

Spiceworks - View Networking - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Inbox | My Profile | My Questions | Logout
Spiceworks has been updated, view release notes
Back New Ticket New Asset Edit
Help Keep Spiceworks Free! Learn more
My Network
Dashboard
My Custom Dash
Inventory
Monitoring
Help Desk
IT Services
Reporting
Settings
My Community
Ask a Question
Discussion Groups
Ratings & Reviews
How-tos
Shared Reports
Whitepapers
Help
Videos
Documentation
Support
My Tools
Google
IT Calendar
Spice Analytics
Sponsored By
mailtrust
Migrate for FREE
9 Networking
Traffic Analysis for Port: 5 Gigabit - Level on sw-core1
These statistics were last updated 1 minute ago, and 'sw-core1' has been up for 3 months.
Previous 30 Hours (15 minute slices)
Previous 8 Days (30 minute slices)
All Data (41 Days - 2 hour slices)
Bytes per second
in
out
Close
sw-core1 (192.168.168
Timeline
General Info
Configuration
Interfaces
Vlans
Notes
Documents
Port: 4 Gigabit - Level enet 16126 12277 up up
Port: 5 Gigabit - Level enet 179299 30085 up up
Port: 6 Gigabit - Level enet 33 683 up up
Port: 7 Gigabit - Level enet 252 830 up up
Port: 8 Gigabit - Level enet 0 0 up down
Port: 9 Gigabit - Level enet 1918 4973 up up
Port: 10 Gigabit - Level enet 8103 10070 up up
Port: 11 Gigabit - Level enet 1811 57514 up up
Port: 12 Gigabit - Level enet 0 0 up down
Rate This Ad
Sponsored Case Study
LifeSize
Learn More

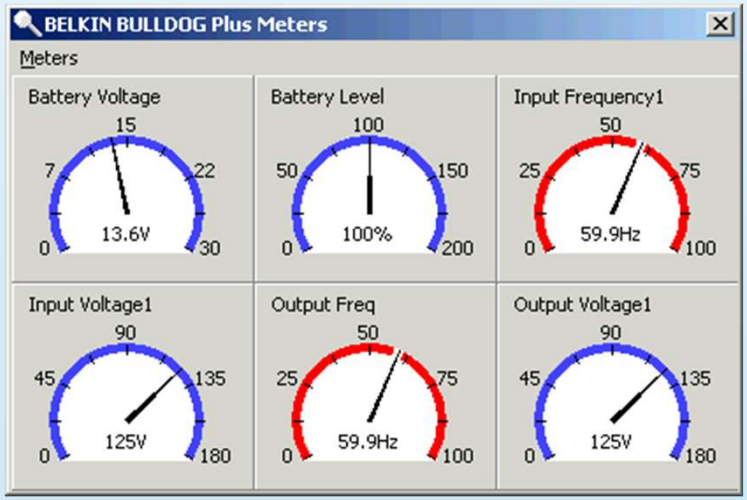
CACTI


« Previous
Showing Rows 1 to 10 of 10
Next »
hp5412zl - Traffic - A1 [5G uplink]
hp5412zl - Traffic - C1 (Torun)
hp5412zl - Traffic - C10 (Shashan)
hp5412zl - Traffic - C17 (WSRT)
hp5412zl - Traffic - C4 [UK1]
hp5412zl - Traffic - C5 (Parkes)
bits per second
Fri 00:00
Fri 12:00

UPSVIEW


UPSView - Version 4.2 (007)
UPS View Functions Logs Help Quit
UPS On
Line Present
On Battery
Battery Low
Bypass On
Overload
Overtemperature
Alarm
Input Voltage
L1 223 V
L2 225 V
L3 225 V
150 V
250 V
Load
L1 15 %
L2 11 %
L3 16 %
0 %
110 %
Battery Capacity
100 %
324 V
0 %
100 %
Autonomy Time
182 min
Output
Bypass Line
Frequency 49.9 Hz 49.9 Hz
Voltage L1 229 V 224 V
Voltage L2 232 V 224 V
Voltage L3 231 V 224 V
UpsAgent running: No
UPS 01: On Line


UPS: Battery charge (percent) (12h)
110 %
100 %
90 %
80 %
70 %
04.08 19:56
20:30
21:00
21:30
22:00
22:30
23:00
23:30
05.08
00:30
01:00
01:30
02:00
02:30
03:00
03:30
04:00
04:30
05:00
05:30
06:00
06:30
07:00
07:30
05.08 07:56
Synology UPS - Battery charge (percent) [avg]
last 100 %
min 79 %
avg 98.69 %
max 100 %
Data from history. Generated in 0.69 sec


BELKIN BULLDOG Plus Meters
Meters
Battery Voltage
15
7
22
0
30
13.6V
Battery Level
100
50
150
0
200
100%
Input Frequency1
50
25
75
0
100
59.9Hz
Input Voltage1
90
45
135
0
180
125V
Output Freq
50
25
75
0
100
59.9Hz
Output Voltage1
90
45
135
0
180
125V

LEANDRO A. ESTRADA

Departamento Informática
Ministerio de Salud

laestrada@entrerios.gov.ar