Apéndice D
Análisis de controles, políticas de uso de red y acceso a internet, encuestas aplicadas y sus resultados

I. Análisis de controles

Vulnerabilidad	Nivel de riesgo	Control sugerido
Red inalámbrica abierta.	Alto	Hotspot, servidor Radius, cifrado.
Inexistencia de controles sobre el uso de la red inalámbrica.	Alto	Hotspot, servidor Radius, cifrado.
Poco control en la administración de direcciones IP.	Alto	Inventario de gestión de direcciones IP.
Inexistencia de control en la información descargada a través de la red de la institución.	Alto	Firewall, filtrado de contenido.
Falta de cuidado del equipo de cómputo.	Alto	Concientización en temas de seguridad.
Limitantes de potencia en UPS.	Alto	Evaluación y adquisición de un UPS.
Falta de mecanismos de control perimetral de la red.	Alto	Firewall, IDS, gestor de uso de red.
Uso de protocolos de administración inseguros.	Alto	Políticas de configuración de equipos activos.
Inexistencia de políticas de uso de red.	Alto	Elaboración de políticas de uso de red.
Inexistencia de políticas para servidores.	Alto	Elaboración de políticas para servidores.
Inexistencia de respaldos en equipos activos.	Alto	Elaboración de políticas de respaldo.
Acceso a todos los recursos de red institucional.	Alto	Firewall perimetral, firewall site de servidores, vlan's, NAT's.
Uso de una misma contraseña por periodos largos de tiempo.	Alto	Políticas de contraseñas.
Uso de una contraseña única en varios equipos.	Alto	Políticas de contraseñas, concientización en temas de seguridad.
Uso de contraseñas no robustas.	Alto	Políticas de contraseñas, concientización en temas de seguridad.
Confianza en otras personas.	Alto	Concientización en temas de seguridad.
Uso de IP's homologadas para usuarios en general.	Alto	Vlan, NAT.
Fallas por parte del proveedor del suministro eléctrico.	Alto	----------
Puertos abiertos sin uso en estación de trabajo.	Alto	Políticas de hardening en estaciones de trabajo.
Inexistencia de respaldos en las diferentes Secretarías.	Medio	Políticas de respaldo.
Tableros eléctricos expuestos.	Medio	Informar de la observación a la Secretaría Administrativa.
Controles de acceso físicos, inseguros para administración de servidores.	Medio	Implementar controles biométricos en los sites.
Vulnerabilidades inherentes del protocolo TCP/IP.	Medio	Políticas de monitoreo.

Vulnerabilidad	Nivel de riesgo	Control sugerido
Daño en hardware por fallas eléctricas.	Medio	UPS.
Inexistencia de control en el tráfico de red generado por la institución.	Medio	Gestor de uso de red.
Fuga de información.	Medio	Políticas de confidencialidad.
Daño físico a la infraestructura de red.	Medio	Cableado estructurado.
Puertos abiertos sin motivo en servidores críticos.	Medio	Políticas de hardening en servidores.
Inexistencia de controles de seguridad en portátiles.	Medio	RFID, bandas magnéticas, cintas de seguridad para portátiles.
Inexistencia de monitoreo de uso de la red.	Medio	Políticas de monitoreo.
Fallas en sistemas de aire acondicionado.	Medio	Mantenimiento preventivo.
Control de acceso débil en aplicaciones.	Medio	Políticas desarrollo de software seguro.
Personal poco capacitado en temas de seguridad.	Medio	Capacitación del personal.
Inexistencia de actualizaciones en terminales de trabajo, servidores, antivirus y equipos de red.	Medio	Políticas de hardening en estaciones de trabajo y Políticas de hardening en servidores.
Falta de mantenimiento preventivo en servidores y equipos activos.	Medio	Mantenimiento preventivo en servidores y equipo activo.
Falta de mantenimiento de estaciones eléctricas.	Medio	Mantenimiento preventivo en estaciones eléctricas.
Falta de corriente eléctrica regulada.	Medio	Implementar reguladores en la mayoría de los equipos.
Inexistencia de fuente de corriente eléctrica alterna.	Medio	Planta eléctrica.
Inexistencia de planes de capacitación.	Medio	Capacitación del personal.
Inexistencia de sites alternos.	Medio	Contratos con compañías o acuerdos con otras instituciones.
Cableado de red expuesto.	Medio	Cableado estructurado.
Respaldos en mismo disco duro.	Medio	Políticas de respaldo.
Parámetros por default en equipos activos.	Medio	Políticas de configuración de equipos activos.
Acceso a todas las terminales de administración.	Medio	Firewall perimetral, firewall Site servidores, listas de control de acceso.
Acceso a todos los recursos de internet.	Medio	Firewall, gestor de contenido.
Uso de protocolos de comunicación inseguros.	Medio	Implementación de comunicaciones cifradas.
Falta de mantenimiento en cableado eléctrico.	Medio	Mantenimiento preventivo en la institución.

Vulnerabilidad	Nivel de riesgo	Control sugerido
Inexistencia de controles de humedad.	Medio	Sensor de humedad.
Inexistencia de controles de temperatura.	Medio	Sensor de temperatura.
Consultas de sitios con software malicioso.	Medio	Gestor de contenido, capacitación al usuario.
Descarga de ejecutables de sitios no confiables.	Medio	Gestor de contenido, capacitación al usuario.
Inexistencia de políticas sobre el uso del equipo de cómputo.	Medio	Políticas sobre el uso del equipo de cómputo.
Autoarranque de dispositivos extraíbles.	Medio	Políticas de hardening en estaciones de trabajo.
Falta de políticas de desarrollo de software seguro.	Medio	Políticas de desarrollo de software seguro.
Inexistencia de controles de integridad en equipos activos.	Medio	Memorias técnicas y respaldos de configuración.
Firmas antivirus deficientes.	Medio	Evaluación y adquisición de un antivirus.
Inexistencia de políticas de uso de software.	Medio	Políticas de hardening en estaciones de trabajo.
Poco control sobre los respaldos.	Medio	Políticas de control de cambios y políticas de respaldo.
Filtrado de agua a Sites.	Medio	Mantenimiento preventivo.
Inexistencia de controles sobre el uso de procesador, memoria, disco duro y ancho de banda.	Medio	Políticas de hardening en servidores.
Falta de procedimientos de creación de cuentas.	Medio	Políticas de contraseñas.
Vulnerabilidades inherentes a las aplicaciones.	Medio	Actualizaciones.
Tiempo de vida útil de los equipos.	Medio	Mantenimiento preventivo, renovación de hardware.
Tuberías expuestas.	Medio	Restructuración de instalación eléctrica, mantenimiento.
Uso de versiones viejas en aplicaciones.	Medio	Actualizaciones.
Vulnerabilidades conocidas en sistemas operativos.	Medio	Actualizaciones.
Empleo de software sin actualizaciones.	Medio	Actualizaciones.
Inexistencia de auditorías.	Bajo	Planificación de auditorías.
Limitantes de espacio en disco duro en servidores.	Bajo	Evaluación y adquisición de medios de almacenamiento masivo.
Fallas eléctricas.	Bajo	Mantenimiento general a la red Eléctrica.
Inexistencia de cultura de seguridad en usuarios finales.	Bajo	Capacitación del personal.
Inexistencia de control perimetral de los puertos permitidos.	Bajo	Firewall perimetral, IDS.
Inexistencia de procedimientos de cambios en sistemas.	Bajo	Políticas de control de cambios.

Vulnerabilidad	Nivel de riesgo	Control sugerido
Inexistencia de políticas en sistemas operativos.	Bajo	Políticas de hardening en estaciones de trabajo.
Inexistencia de cifrado en discos duros.	Bajo	Cifrado.
Poca separación de funciones críticas.	Bajo	Definir responsabilidades, separación de funciones.
Dispositivos extraíbles sin cifrado.	Bajo	Cifrado.
Fallas por parte del proveedor de servicios de internet.	Bajo	Enlaces redundantes, acuerdos de LSA.
Daños en la configuración de los equipos por poco mantenimiento.	Bajo	Mantenimiento preventivo.
Descuido en el manejo del hardware.	Bajo	Capacitación del personal.
Errores de cambios en la configuración de equipos activos y servidores.	Bajo	Capacitación del personal.
Inexistencia de control a servicios de servidores.	Bajo	Políticas de hardening en servidores.
Inexistencia de políticas de confidencialidad.	Bajo	Políticas de confidencialidad.
Inexistencia de monitoreo de las aplicaciones.	Bajo	Políticas de monitoreo, implementación de herramientas de monitoreo.
Poca educación sobre seguridad a usuarios finales.	Bajo	Capacitación del personal.
Errores humanos.	Bajo	Capacitación del personal.
Aprovechamiento de vulnerabilidades de controles físicos.	Bajo	Implementación de controles de acceso de 2 o más factores.
Falta de gestión de garantías.	Bajo	Adquisición de periodos de garantía más largos.
Interferencias magnéticas.	Bajo	----------
Desastres naturales en la institución.	Bajo	Prevención.

II. Políticas de uso de red y acceso a internet

Objetivo del documento

Definir los criterios normativos para implementar, preservar y hacer uso eficiente, racional y correcto de los recursos de red.

Alcance

Al utilizar la red de datos del Colegio de Ciencias y Humanidades se espera que el usuario (académico, administrativo, estudiante) use los servicios con respeto, responsabilidad.

La aplicación y seguimiento de las siguientes políticas, serán supervisadas y aplicadas por la Secretaría de Informática.

Definiciones

1. Red DGCCH: nombre dado al conjunto de instalaciones y recursos informáticos que conforman parte de la infraestructura de telecomunicaciones.
2. Usuario: Se entiende por usuario de la red, todo ente que reciba o provea información a través de la Red DGCCH.
3. Servicio: Se entiende por servicio, los aplicativos y/o conjunto de programas que apoyan la labor académica y administrativa del quehacer cotidiano de los usuarios.
4. Cuenta: Mecanismo de identificación asignado a un usuario, dicho mecanismo será personal, único e intransferible, vigente durante el tiempo de vinculación del usuario con la Institución.
5. SG: Acrónimo de Secretaría General.
6. SA: Acrónimo de Secretaría Administrativa.
7. Monitoreo: Estadísticas de uso de red y verificación de que los paquetes de datos estén formados adecuadamente.

Generalidades

La UNAM, a través de la Secretaría de Informática, encargada de cómputo y redes de datos del plantel o dirección del Colegio de Ciencias y Humanidades, brindará a la comunidad académica, administrativa y estudiantil el servicio de acceso a la red para la navegación en internet, servicios adicionales sobre la misma y consulta de correo electrónico, como un recurso de apoyo a la labor académica, de investigación, difusión cultural y actividades administrativas. Los académicos, empleados y alumnos deben emplearlos para su trabajo y estudio.

Toda persona que utilice los servicios que ofrece la red de datos de la Dirección General del Colegio de Ciencias y Humanidades deberá conocer y apegarse a las políticas vigentes de uso de red, el desconocimiento del mismo no exonera de las responsabilidades asignadas. Quedan explícitamente prohibidas todas aquellas actividades que no estén expresamente permitidas en este documento.

Emisión y modificación de normas

La Secretaría de Informática, con previa autorización de la Secretaría General, Secretaría Administrativa y Junta de directores del Colegio de Ciencias y Humanidades, tiene la facultad de crear, modificar y emitir nuevas políticas de uso de la red que son aplicables a todos los usuarios.

De la información transportada en la Red

La Secretaría de Informática de la Dirección General del Colegio de Ciencias y Humanidades, no controla ni es responsable del contenido y veracidad de la información que se transporta en la red, en consecuencia los usuarios aceptan utilizar el servicio de comunicación sólo para enviar y recibir mensajes e información.

El acceso al contenido publicado en internet, archivos descargados, programas ejecutados desde Internet, mensajes recibidos y demás información que pueda estar en Internet es susceptible de contener malware. Por lo anterior es responsabilidad del usuario, ingresar sólo a sitios que considere seguros.

Personal autorizado

Están autorizados a utilizar los servicios de red de la DGCCH todo el personal que se encuentre en la siguiente clasificación.

- Académicos del Colegio de Ciencias y Humanidades.
- Personal administrativo.
- Personas que presten servicios a la institución de manera directa.
- Personal de apoyo institucional.
- Administradores de servicios.
- Becarios.
- Alumnos.

Responsabilidades de los administradores de red y cómputo

Se definen como administradores de red y cómputo a:

- Secretaría de Informática para Dirección General del Colegio de Ciencias y Humanidades.
- Encargados de cómputo y telecomunicaciones definidos en cada plantel.

Dentro de sus responsabilidades se contemplan los siguientes puntos.

- Realizar y vigilar que sean cumplidas las políticas de uso de red y acceso a internet.
- Llevar un control y resguardo de los recursos informáticos del plantel o dirección general.
- La configuración y asignación de direcciones IP.
- Instalación y administración de equipos activos de red.

- Desarrollar estrategias que permitan el control de las diferentes aulas, centros de cómputo y recursos informáticos del plantel.
- Mantener en funcionamiento los servicios que les corresponde administrar, en caso de alguna falla se realizará un informe detallado del problema presentado.
- Monitoreo del tráfico de la red de datos.
- Informar a los usuarios sobre el funcionamiento y la forma como debe ser utilizado.
- Informar a los usuarios sobre cambios de la suspensión temporal y/o mantenimiento de los servicios.
- Prestación de soporte técnico en materia, de instalación, configuración y mantenimiento de los equipos de cómputo e infraestructura de red.
- Gestionar y autorizar la solicitud de dominios, subdominios en nic.unam.mx.
- Actualización de la contraseña de correo "cch.unam.mx", sólo la Secretaría de Informática de la Dirección General del Colegio de Ciencias y Humanidades realiza este proceso.

De los recursos

- El servicio de conexión a la red, estará disponible las 24 horas del día, los 365 días del año. Salvo en situaciones de fuerza mayor, o por cortes parciales o interrupciones relativas al mantenimiento preventivo o correctivo de los equipos y elementos relacionados a la prestación del servicio de Internet.

- La infraestructura de red de la DGCCH, se utilizará únicamente para desarrollos académicos, de investigación, técnicos y administrativos de la institución, así mismo sólo podrán ser usados de acuerdo con lo previsto por las especificaciones de cada dispositivo.

- Se prohíbe, salvo autorización escrita y supervisión de la Secretaría de Informática de la DGCCH, la intervención física de los usuarios sobre los recursos de la red (cables, enlaces, equipos activos y/o pasivos) y el acceso a los centros de cableado de los edificios.

- Sólo la Secretaría de Informática de la Dirección General del Colegio de Ciencias y Humanidades, está facultado para conceder acceso a los recursos y/o servicios de la red.

- Todos los usuarios con recursos de cómputo bajo su responsabilidad, sólo harán uso de los mismos en beneficio de la institución, deberán velar por la protección física de los mismos.

- Sólo el personal debidamente autorizado por la Secretaría de Informática, podrá modificar la configuración y conexión física de los equipos de telecomunicaciones de la institución.

Usos inaceptables

Queda prohibido.

- Cambiar parámetros de red configurados en su equipo de cómputo.
- Transmisión de información de terceros, sin previa autorización de la autoridad competente.
- Transmisión de contenido pornográfico.
- Distribución no autorizada o copia de software sin licencia.

- Distribución de información de carácter comercial o cualquier otra forma, que represente un lucro para la persona que la origina.
- Distribución de material obsceno o que incite la violencia.
- Envío de correos no solicitados en un alto volumen (spam).
- Usar programas "peer to peer" (P2P) o alguna otra tecnología que permita el intercambio de archivos en volumen.
- Publicación de material electrónico con derechos de autor, sin previa autorización por escrito de su titular.
- Propagación de código malicioso, virus, gusanos, spyware, etcétera.
- Exploración no autorizada de los servidores.
- Acoso informático y/o electrónico a cualquier miembro o usuario de la red.
- Atacar a otros usuarios por cualquier medio (negación de servicio, phising, pharming, fuerza bruta, etcétera.).
- Atentar contra la disponibilidad, integridad, confidencialidad de la red.
- Extender el alcance de la red a más equipos por medio de cualquier dispositivo físico o lógico (NAT, túneles, switch, hub, ruteador, conexiones compartidas, etcétera.).
- Montar servidores sin previa autorización por escrito, al área de cómputo encargada de la administración de red de la Dirección General o planteles, según sea el caso.
- Utilizar los recursos de la red para juegos online.
- Transgredir cualquier recurso computacional, sistema o sitios de telecomunicaciones a los que está permitido acceder.

De los derechos y responsabilidades de los usuarios de red

- Es responsabilidad de los empleados que tengan personal a su cargo: la difusión y el apego a las políticas.
- Mantener en óptimas condiciones el equipo, accesorios y demás dispositivos de cómputo que se les haya asignado.
- Solicitar por escrito a los responsables de red, la asignación de una dirección IP y los servicios que en su caso brindará, dicho equipo.
- Reportar inmediatamente el robo o extravío de algún equipo.
- Reportar a los administradores de red, el daño de nodos de red que se encuentren localizados en su área de trabajo.
- Respetar la configuración de los equipos de cómputo que se les asignen.
- Mantener la confidencialidad de sus cuentas de acceso.
- Utilizar los recursos de red, con las limitantes consignadas en el punto de usos inaceptables.
- Es responsabilidad del usuario, el tipo de información al cual accede, ya que ésta puede ser contenido inapropiado.
- Realizar el respaldo de su información.

- Los usuarios gozan de la privacidad de su información, con la salvedad de aquellos casos en que se detecten acciones que pongan en riesgo la seguridad de la red de la DGCCH o de cualquier otra red.
- Cualquier cambio en el hardware de red en un equipo de cómputo, deberá ser notificado en un lapso no mayor a 4 días a la Secretaría de Informática.
- La Secretaría de Informática, se reserva el derecho de cancelar temporalmente o definitivamente el servicio, con previa notificación al usuario, cuando se haga uso inapropiado de la red, dentro de las actividades especificadas en usos inapropiados.

Monitoreo de comunicaciones

A solicitud escrita de la autoridad competente o cuando exista alguna orden judicial para responder ante procesos legales, la Secretaría de Informática proporcionará la información transmitida en la Dirección General del Colegio de Ciencias y Humanidades y que esté disponible para su acceso de conformidad con las leyes aplicables.

El usuario al momento de utilizar la red de la Dirección General del Colegio de Ciencias y Humanidades, conoce y manifiesta su consentimiento para que la Secretaría de Informática realice monitoreo en su conexión, cuando lo juzgue necesario, únicamente con el propósito de mantener la integridad y operación efectiva de los equipos de telecomunicaciones o cuando responda a un requerimiento de las autoridades administrativas o judiciales.

III. Encuesta administradores

ANÁLISIS DE RIESGO CON BASE EN EL NIST 800-30, 800-53
ADMINISTRADORES

Institución	Dirección General del Colegio de Ciencias y Humanidades
Nombre:	
Secretaría a la que pertenece:	
Fecha	Firma

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Controles de Seguridad

1. Se tiene definidas políticas de confidencialidad, para la información que maneja.
   SÍ ☐ NO ☐
2. Conoce si existen dispositivos de seguridad y monitoreo de la red en su institución, si su respuesta es afirmativa indique los elementos que identifica.
   SÍ ☐ NO ☐
3. Se tienen definidas políticas de respaldos en los equipos que administra, si la respuesta es afirmativa indique la frecuencia de respaldo.
   SÍ ☐ NO ☐
4. En los dispositivos que administra, aplica algún esquema de políticas de seguridad, si la respuesta es afirmativa indique qué puntos cubre.
   SÍ ☐ NO ☐
5. Cuenta la institución con un documento oficial de Políticas y Procedimientos de Seguridad de la Información.
   SÍ ☐ NO ☐
6. En caso de existir un documento de políticas de seguridad, indique cuáles de los siguientes aspectos hacen parte de su contenido:

Descripción	SÍ	NO
Objetivos de las políticas		
Normas y políticas a ser implementadas		
Definición de responsabilidades en la gestión de la seguridad		
El manejo de los incidentes relacionados con la seguridad de la información		
Referencias a la información que soporte las políticas de seguridad		

7. En caso de existir un documento de políticas de seguridad, el mismo ha sido publicado y comunicado a todos los empleados y contratistas de la institución.

SÍ		NO	

Organización de la Seguridad

8. Existe en la institución una estructura de personal y recursos que permita la implementación y control de las políticas de seguridad de la información.

SÍ		NO	

Gestión de Activos de Información

9. Existe en la institución un inventario detallado de activos que incluya la información del activo, como tipo de activo, ubicación, formato, información de soporte y mantenimiento, licencias y valor para el negocio, su responsable o dueño designado, etcétera.

SÍ		NO	

10. Si la respuesta a la pregunta No. 1 fue un "SÍ", se tiene una clasificación de activos con base en la necesidad, las prioridades y el grado esperado de protección del activo de información.

SÍ		NO	

Seguridad de los Recursos Humanos

11. Se han revisado todas las posiciones y cargos en función de las responsabilidades en materia de seguridad de la información.

SÍ		NO	

12. Existen documentos tales como manuales de procedimientos que reflejen de manera precisa los roles y responsabilidades para cada cargo.

SÍ		NO	

13. Las tareas críticas y más sensibles son distribuidas entre varios funcionarios.

SÍ		NO	

14. Existen procedimientos escritos para la contratación, transferencia y terminación de contratos de funcionarios.

SÍ		NO	

15. Se han firmado acuerdos o contratos de confidencialidad con todos los funcionarios y contratistas que manejan información sensible.

SÍ		NO	

Seguridad Física y del Entorno

16. El acceso a las instalaciones que albergan información vital, tales como Centros de Cómputo, site de servidores y bodegas de cintas, es controlado y restringido por guardias de seguridad, tarjetas de proximidad, claves de acceso o controles biométricos de acceso, o algún otro, indique cual.

SÍ		NO	

17. Las instalaciones que albergan información vital, cuentan con controles de adecuados, tales como muros, y puertas con seguridad.

SÍ		NO	

18. Las claves de acceso son revisadas y cambiadas con una periodicidad determinada, si la respuesta es afirmativa indique la frecuencia de cambio.

SÍ		NO	

19. Existen procedimientos de revisión periódica de las listas de personal con acceso a instalaciones que albergan información vital.

SÍ		NO	

20. Los visitantes a las áreas que albergan información vital son registrados y escoltados.

SÍ		NO	

21. Los sistemas de detección y extinción de incendios se encuentran correctamente instalados y en operación.

SÍ		NO	

22. Los sistemas de Aire Acondicionado se encuentran correctamente instalados y en operación.

SÍ		NO	

23. Cuenta la institución con un sistema de suministro no interrumpido de potencia o UPS (Uninterruptible Power Supply) que respalde la totalidad de equipos de cómputo, servidores y equipos de comunicaciones de la institución.

SÍ		NO		Parcialmente	

24. Los monitores de los equipos de cómputo están localizados para evitar el acceso y visualización de personas no autorizadas.

SÍ		NO	

25. Los sistemas de cableado estructurado y eléctrico están protegidos contra interceptaciones y daños.

SÍ		NO	

Gestión de Operaciones y Comunicaciones

26. Existe un procedimiento de control de cambios a nivel de los sistemas de procesamiento de información.

SÍ		NO	

27. Se tienen claramente definidos y separados, ambientes de desarrollo, ensayo y operación para los sistemas de procesamiento de información.

SÍ		NO	

28. Se hace la planeación de capacidad para los sistemas de procesamiento de información.

SÍ		NO	

29. Se tiene implementado un sistema de protección contra código malicioso que cubra la totalidad de activos de información.

SÍ		NO	

30. Se tienen implementados sistemas y procedimientos de respaldo o backup para los sistemas que usted administra.

SÍ		NO	

31. Para controlar la seguridad de la red, se tienen implementados sistemas de autenticación.

SÍ		NO	

32. Para controlar la privacidad de la información de la red, se tienen implementados sistemas de cifrado.

SÍ		NO	

33. Existe en los equipos que administra firewall de host. Por favor indique la cantidad.

SÍ		NO		Cantidad	

34. Existe en su institución firewall perimetral. Por favor indique la cantidad existente.

SÍ		NO		Cantidad	

35. Especifique el tipo de tecnología utilizada por el(los) firewall(s).

Firewall basado en hardware dedicado	
Firewall basado en software para Servidor	

36. Marque con una "X" las redes protegidas mediante puertos independientes en el(los) firewall(s) de su institución.

Host	
Red LAN	
Red WAN	
Extranet	
DMZ	

37. Cuenta su institución con Sistemas de Detección de intrusos – IDS.

SÍ		NO	

38. Cuenta su institución con equipos de monitoreo de red, si su respuesta fue afirmativa indique qué dispositivos.

SÍ		NO	

39. Se realiza bloqueo de algunos sitios en el segmento de red.

SÍ		NO	

40. Cuenta su institución con equipos concentradores de VPN´s

SÍ		NO	

Control de Acceso

41. Existen sistemas de control capaces de detectar intentos de acceso no autorizados.

SÍ		NO	

42. Las estaciones de trabajo se desconectan o los salva pantallas protegidos por contraseña se activan después de un periodo determinado de inactividad.

SÍ		NO	

43. Las cuentas de usuario no activas son removidas cuando no se requieren.

SÍ		NO	

44. Si se manejan sistemas de cifrado, existen procedimientos para generación de claves, almacenamiento, uso y destrucción de las mismas.

SÍ		NO	

45. Los parámetros por defecto suministrados por los fabricantes han sido cambiados por parámetros de configuración más seguros.

SÍ		NO	

46. Existen procedimientos para mantener y revisar los logs de actividad de red.

SÍ		NO	

Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

47. Para la adquisición de infraestructura de hardware y software, se realizan documentos detallados de especificaciones técnicas.

SÍ		NO	

48. Se tiene un procedimiento de control de versiones.

SÍ		NO	

49. Se tienen restricciones en sitio para quienes realizan actividades de mantenimiento y reparación.

SÍ		NO	

Gestión de Incidentes de Seguridad

50. Existe un procedimiento para el reporte de incidentes de seguridad.

SÍ		NO	

51. Existe un procedimiento de seguimiento y control de los incidentes de seguridad hasta que los mismos son resueltos.

SÍ		NO	

52. La institución cuenta con personal entrenado para identificar y resolver incidentes de seguridad.

SÍ		NO	

53. La institución cuenta con un plan de continuidad, contingencia y recuperación ante desastres.

SÍ		NO	

54. El plan de continuidad es revisado y probado periódicamente.

SÍ		NO	

55. El plan de continuidad de la institución tiene en cuenta los aspectos relacionados con la seguridad de la información.

SÍ		NO	

Gestión y Procedimientos

Documentación

A nivel de seguridad de la información, existe en su institución documentación de:
Marque con una "X", en caso de existir.

Documento de políticas, normas y procedimientos de seguridad de la Información.	
Documento de evaluación y análisis de riesgos.	
Diagramas de topología de seguridad perimetral.	
Reglas de seguridad.	

¿Cuál es el porcentaje de actualización de la documentación de seguridad de la información en su institución? Marque con "X" su elección.

Porcentaje de actualización de la documentación	Menos de 25%	Entre 25% y 50%	Entre 50% y 80%	Más de 80%
Documento de políticas, normas y procedimientos de seguridad de la Información.				
Documento de evaluación y análisis de riesgos.				
Diagramas de topología de seguridad perimetral.				
Reglas de seguridad.				

¿Cuáles de las siguientes actividades relacionadas con el Sistema de Gestión de Seguridad de la información se realizan en su institución? En caso de indicar que sí se lleva a cabo la actividad, marque con "X" en el campo que más se asemeje a su periodicidad.

Ítem	Actividades	¿Esta actividad se ejecuta actualmente en su institución? (SÍ / NO)	Periodicidad				
			Diario	Mensual	Trimestral	Semestral	Anual
Actividades de operación y configuración							
3.1	Monitoreo de equipos de seguridad Firewalls.						
3.2	Monitoreo de equipos de seguridad sistemas de detección de intrusos.						
3.3	Cambios en la configuración de los equipos de seguridad.						
Actividades de soporte técnico y mantenimiento							
3.4	Monitoreo y gestión de incidentes de seguridad.						
3.5	Generación de reportes de incidentes de seguridad.						
3.6	Mantenimiento preventivo de equipos de seguridad.						
3.7	Mantenimiento correctivo (reparaciones y arreglos) de equipos de seguridad.						
3.8	Administración de garantías) de equipos de seguridad.						
3.9	Gestión de inventarios de activos de información.						
Actividades de medición y análisis							
3.10	Medición y control de incidentes de seguridad.						
3.11	Monitoreo y revisión de logs de seguridad.						
3.12	Revisión del cumplimiento de las políticas de seguridad.						
3.13	Auditoría del Sistema de Gestión de Seguridad de la Información.						

Ítem	Actividades	¿Esta actividad se ejecuta actualmente en su institución? (SÍ / NO)	Periodicidad				
Actividades de planeación							
3.14	Evaluación y revisión del plan de tratamiento de riesgos.						
3.15	Definición y revisión del plan de continuidad de la organización.						
Actividades de capacitación y entrenamiento							
3.16	Entrenamiento para el personal en la operación del sistema de gestión de seguridad.						
Gestión de Servicios							
3.17	Proceso de gestión de incidentes y mesa de ayuda.						
3.18	Proceso de gestión de problemas.						
3.19	Proceso de gestión de configuraciones, cambios y liberaciones.						
3.20	Gestión de niveles de servicio.						
3.21	Medición del factor de calidad del servicio.						

Indique las herramientas con las que su institución cuenta actualmente para realizar las actividades de gestión de seguridad de información.

	Herramienta utilizada
Monitoreo de incidentes de seguridad.	
Administración y configuración de equipos de seguridad.	
Gestión de inventario de activos.	

Identificación de servidores

Si es responsable de algún servidor o servidores favor de llenar la siguiente tabla con los datos correspondientes.

	Servidor 1	Servidor 2	Servidor 3
Dirección IP			
Sistema operativo			
Servicios			
Puertos			
Nombre del Host			
Cuenta con memoria técnicas Sí o No			
Frecuencia con la que realiza los ~~de~~ respaldos			
Considera que su equipo es seguro Sí o No			
Conoce el término hardening Sí o No			
Qué controles aplica para garantizar un nivel de seguridad			

IV. Encuesta usuarios

ANÁLISIS DE RIESGO CON BASE EN EL NIST 800-30, 800-53
USUARIO

Entidad	Dirección General del Colegio de Ciencias y Humanidades
Nombre:	
Secretaría a la que pertenece:	
Fecha:	Firma

I. Identificación y evaluación de activos

1. Describa las principales actividades que realiza.

2. Definir los principales activos con los que se cuenta; entendiendo como un activo aquello que tiene valor para el departamento y que requiere protección.

	Activos
Hardware (equipo de cómputo físico)	
Software (aplicaciones para realizar su trabajo)	
Sistemas (aplicaciones adicionales)	
Datos e Información	
Personal	

Con base en los activos citados anteriormente indicar el grado de importancia (valor), mediante una X. (En caso de requerirlo anexe una hoja para sus repuestas)

ACTIVOS	Muy importante	Importante	Medianamente importante	Sin importancia

3. Cuál es la forma de almacenamiento para la información manipulada por su departamento. Enumérela con base en el orden de uso. (En caso de emplear otras formas mencione y escriba brevemente).

- ☐ Disco duro.
- ☐ Archivero.
- ☐ CD, DVD, Blue Ray.
- ☐ Diskette.
- ☐ Cintas magnéticas.
- ☐ Cuarto especial para almacenar información.
- ☐ USB.
- ☐ Otro:_____

4. Considera que los medios de almacenamiento para la información, implementados en el departamento son seguros. Justifique su respuesta.

SÍ ☐ NO ☐ Parcialmente ☐

II. Identificación y descripción de amenazas

1. La gente con quién labora, tiene conocimientos acerca de los temas relacionados con la seguridad de la información.

SÍ ☐ NO ☐ Parcialmente ☐

2. Indique con qué frecuencia se presentan las siguientes situaciones marcando con una “X”, la situación que más se acerque a la realidad de su organización. (En caso de presentarse suceso diferente a los listados en la siguiente tabla, mencione y describa brevemente).

Suceso	Muy probable	Probable	Poco probable	Probabilidad nula
Robo de información.				
Ex empleados que hayan tenido acceso a la información sin autorización.				
Extravío de información por descuido del personal que la manipula.				
Alteración de información por personal no autorizado.				
Fallas en los dispositivos donde almacene información.				
Lentitud en la respuesta cuando se trabaja con la red.				
Denegación de los servicios brindados por la RED implementada en la institución.				
Falta de mantenimiento en el cableado de red.				
Desastres naturales que dañen equipo de la institución.				
Personal ajeno al departamento que haya intentado recabar información por medio del personal que labora dentro de su departamento.				
Infección de los equipos de cómputo (virus, gusanos, spyware, malware en general).				
Modificación en la configuración de red de sus equipos, por terceros.				
Fallas en los equipos de cómputo.				
Fallas eléctricas.				
Robo de equipos de cómputo, que contenga información de la institución.				
Acceso no autorizado a la información.				
Revelación de información confidencial por el personal que lo manipula.				
Copias no autorizadas de la información.				
Desconfiguración del sistema o de los dispositivos con los cuales se manipula la información.				
Personas que hayan aceptado un soborno y brindado información confidencial.				
Accidentes por desconocer las políticas de seguridad o (inexistencia de políticas).				
Falta de conocimiento técnicos para realizar alguna tarea.				
Otros.				

3. Si se presentaran cualquiera de las situaciones anteriores, qué sucedería en el departamento.

4. ¿Se cuenta con algún método de control de acceso a la información? Describa brevemente en qué consiste.

Password ☐ Tarjeta electrónica ☐ Certificados electrónicos ☐
Cerradura ☐ No ☐ No sé ☐ Cifrado ☐

III. Identificación y descripción de vulnerabilidades

1. Existen procedimientos establecidos que indiquen como realizar un respaldo de información en su área.

SÍ		NO		NO SÉ	

2. Se cuenta con respaldo de la información.

SÍ		NO		NO SÉ	

3. Dispositivos empleados para llevar a cabo el respaldo de la información (Puede seleccionarse más de una opción), en caso de tener otro tipo mencione y describa brevemente) enumere de mayor a menor, en caso de no utilizar colocar 0.

☐	Cintas magnéticas.	
☐	Folder -> (Archivero).	
☐	CD, DVD, Blue Ray.	
☐	Diskette.	
☐	Discos duros.	
☐	USB.	
☐	Otro.	

4. La información contenida en su equipo de cómputo está protegida con contraseña.

SÍ		NO		NO SÉ	

5. la información contenida en su equipo de cómputo se encuentra cifrada (emplea dos contraseñas para iniciar sesión en su equipo).

SÍ		NO		NO SÉ	

6. Las contraseñas que emplea son cambiadas con una periodicidad determinada.

SÍ		NO		NO SÉ	

7. El personal que ingresa a la institución se identifica al ingresar a la misma.

SÍ		NO		NO SÉ	

8. Existen bitácoras del personal que ingresa al a institución.

SÍ		NO		NO SÉ	

9. Se cuenta con antivirus actualizados en los equipos de cómputo.

SÍ		NO		NO SÉ	

10. Se realizan actualizaciones del sistema operativo en su equipo de cómputo.

SÍ		NO		NO SÉ	

11. Se cuenta con corriente eléctrica regulada en la instalación.

SÍ		NO		NO SÉ	

12. Se cuenta con "no break" para el cuidado de los equipos.

SÍ		NO		NO SÉ	

13. Se da mantenimiento preventivo a los equipos de cómputo a su cargo.

SÍ		NO		NO SÉ	

14. Las instalaciones están en condiciones adecuadas para el resguardo del equipo y de la información. En caso de responder NO especificar las problemáticas que tienen las instalaciones.

SÍ		NO		NO SÉ	

15. Con qué frecuencia se va la luz dentro del departamento. Indique el número de veces al mes (aproximado).

SÍ		NO	

16. Se cuenta con políticas de uso de red para la institución.

SÍ		NO		NO SÉ	

17. Se cuentan con políticas de seguridad particulares para su departamento.

SÍ		NO		NO SÉ	

18. Se cuentan con chapas que resguarden la seguridad de las oficinas que integran el departamento.

SÍ		NO		NO SÉ	

19. Se cuentan con extinguidores para incendios.

SÍ		NO		NO SÉ	

20. Al instalar o emplear un equipo nuevo, se leen los manuales adjuntos al equipo.

21. Considera adecuada la administración de la RED implementada, en caso de ser negativa la respuesta, describir cuál es la problemática que se tiene con la administración de la red.

SÍ		NO	

22. Se permite el acceso a cualquier persona a su departamento.

SÍ		NO	

23. Cómo se controla el acceso de personas dentro del departamento.

24. Se cuenta con pararrayos en la estructura física de la institución.

SÍ		NO		NO SÉ	

25. Existe filtrado de agua en su departamento, si la respuesta es "sí" indique el lugar.

SÍ		NO		NO SÉ	

26. En caso de un temblor, ¿Cómo se puede recuperar la información, cuando se haya dañado el edificio?

_____

27. Se cuenta con algún mecanismo de autenticación en la red inalámbrica de su institución.

SÍ		NO		NO SÉ	

28. Conoce si existen herramientas implementadas en la institución que garanticen o aumenten la seguridad de su equipo de cómputo.

SÍ		NO		NO SÉ	

29. Conoce si existe monitoreo de la seguridad de su red, en caso de ser "sí" su respuesta coloque el nombre del mecanismo que conoce.

SÍ		NO		NO SÉ	

IV. Identificación de controles

1. Cuando la información ha sufrido un ataque, qué consecuencias se han presentado. Enumérelas en orden de mayor (4) a menor (1) frecuencia de haber ocurrido:

Situación	Ocurrencia
La información es accedida por usuarios no autorizados.	
Se han realizado modificaciones de la información del departamento y esta información ha perdido su estado original.	
Se ha perdido de forma irreparable la información debido al ataque y no se pudo recuperar.	
Debido al ataque se han perdido temporalmente los servicios.	

2. Qué medidas ha tomado usted para el control de la seguridad en el área donde labora (Describa brevemente su área y sus funciones en ella).

3. Conoce qué medidas ha tomado el administrador de la RED del departamento para la protección de la seguridad de la institución.

4. La institución cuenta con controles de acceso físicos a los equipos de cómputo y elementos de red.

SÍ ☐ NO ☐ CUÁLES:_____

V. DETERMINACIÓN DE RIESGOS RESIDUALES

1. Considera necesario e importante el contar con respaldos de la información que maneja su departamento.

SÍ ☐ NO ☐ NO SÉ ☐

2. Realiza respaldo de la información que maneja.

SÍ ☐ NO ☐

Con qué frecuencia:_____

3. Tiene conocimiento de la existencia de programas antivirus, si su respuesta a la pregunta anterior fue afirmativa cual conoce.

SÍ ☐ NO ☐ NO SÉ ☐

4. ¿Cuenta con nombre de usuario y contraseña para ingresar al equipo?

SÍ ☐ NO ☐

5. Usted puede instalar cualquier programa en su equipo sin restricción alguna.

SÍ ☐ NO ☐ NO SÉ ☐

6. ¿Qué sistema operativo maneja en su equipo de cómputo?

Windows XP ☐ UNIX ☐
Windows 2000 ☐ Linux ☐
Windows Vista ☐ Otro:_____
Windows 7 ☐
Windows server 2003 ☐
Windows server 2008 ☐

7. Cuenta el equipo que maneja con un firewall personal:

SÍ ☐ NO ☐ NO SÉ ☐

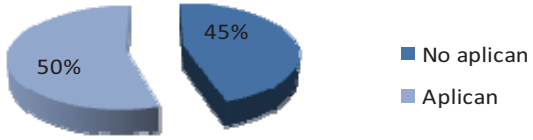
8. Aplica las actualizaciones que se liberan para sus aplicaciones y sistema operativo.

SÍ ☐ NO ☐ Parcialmente ☐

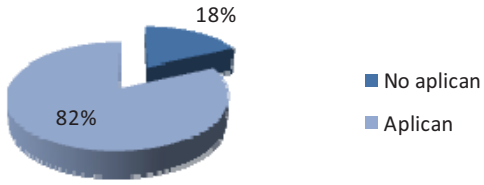
9. ¿Qué tipo de uso le da a Internet?

V Resultados encuestas administradores

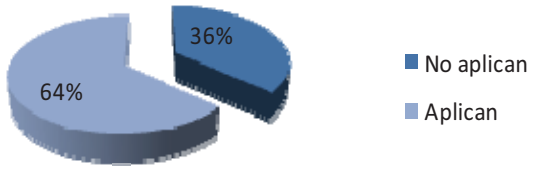
Políticas de confidencialidad



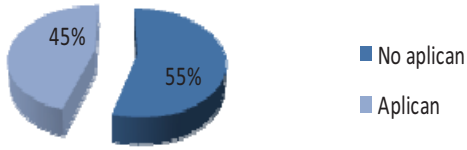
Existencia de dispositivos de seguridad



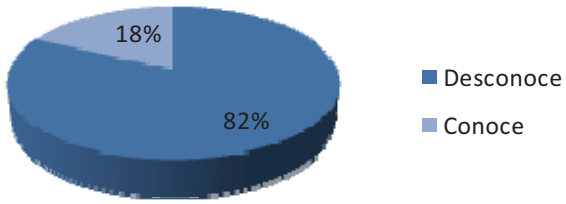
Políticas de respaldo en los equipos que administra



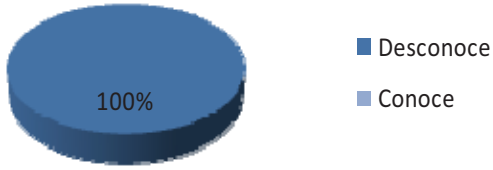
Políticas de seguridad en los equipos que administra



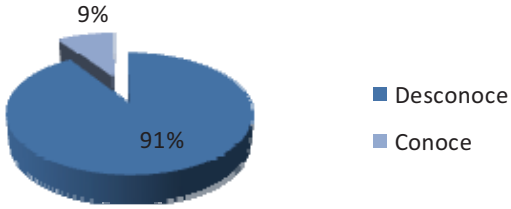
Existencia políticas de seguridad



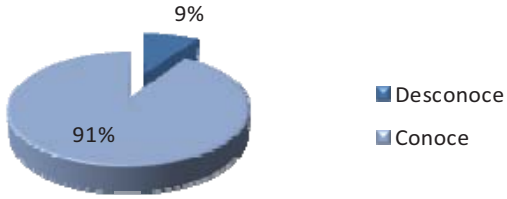
Conocen los puntos de las políticas

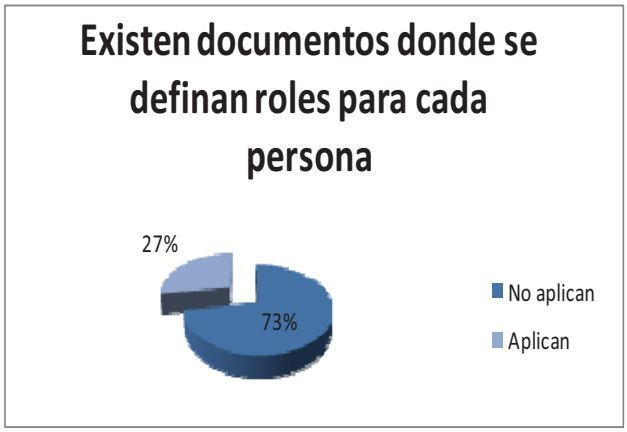


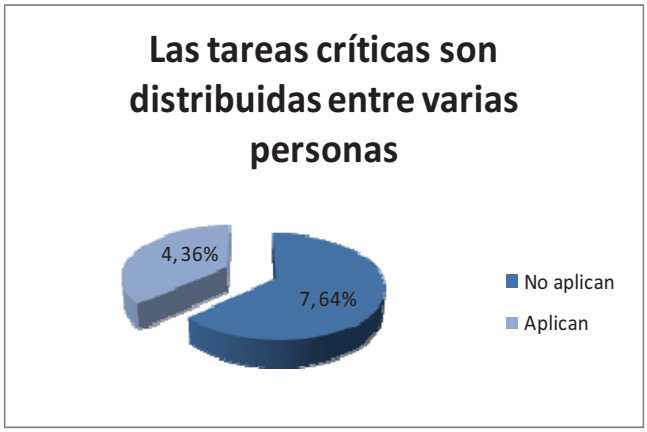
Se han publicado las políticas

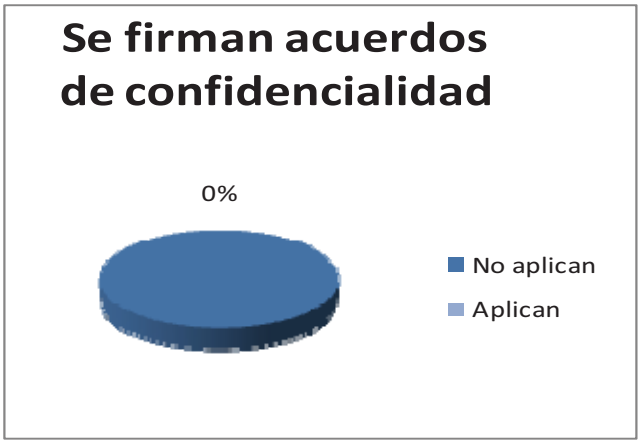


Existe una estructura de personal que permita la implementación de políticas

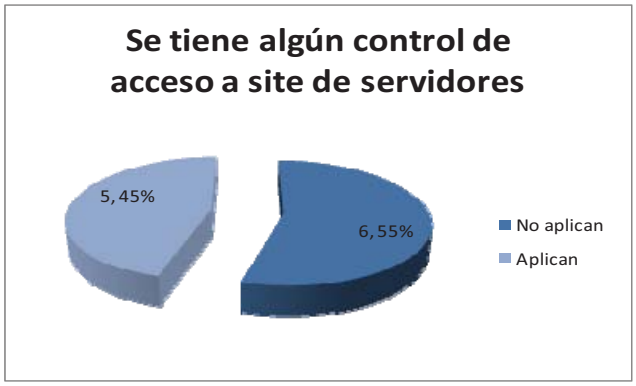






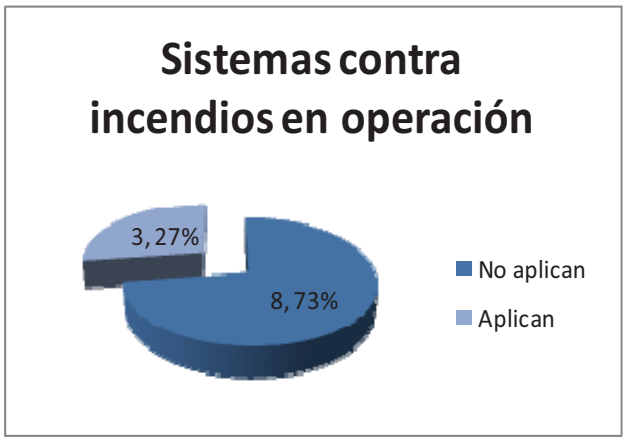


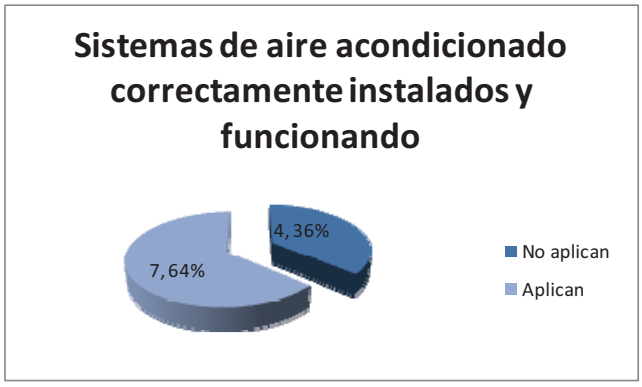
Nota: "0%" del personal firma acuerdos de confidencialidad

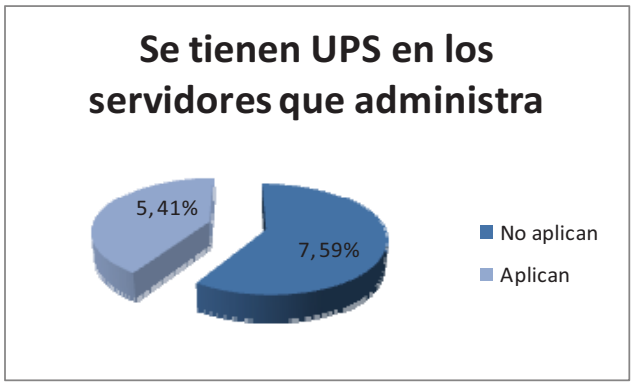

Se tiene algún control de acceso a site de servidores
5, 45%
6, 55%
No aplican
Aplican


Se tienen muros y puertas de seguridad
2, 18%
9, 82%
No aplican
Aplican

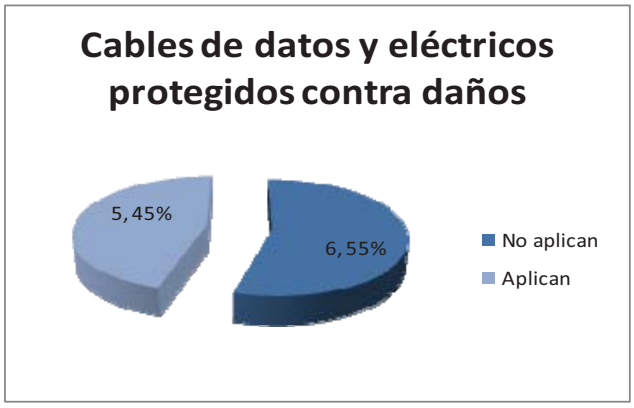

Los visitantes son registrados y escoltados
1, 9%
10, 91%
No aplican
Aplican

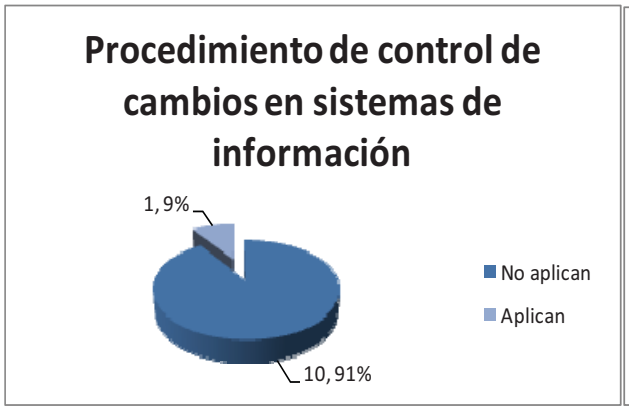

Sistemas contra incendios en operación
3, 27%
8, 73%
No aplican
Aplican

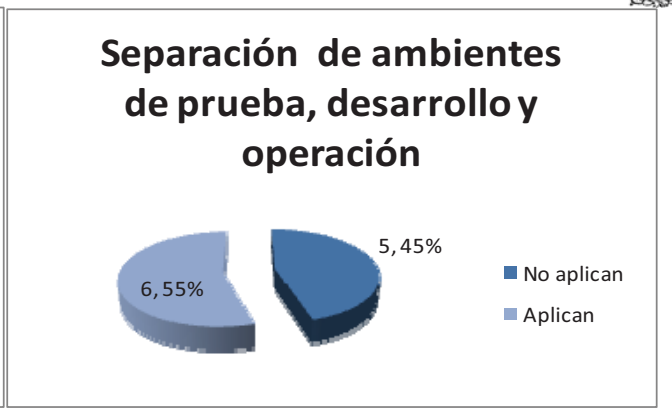

Sistemas de aire acondicionado correctamente instalados y funcionando
4, 36%
7, 64%
No aplican
Aplican

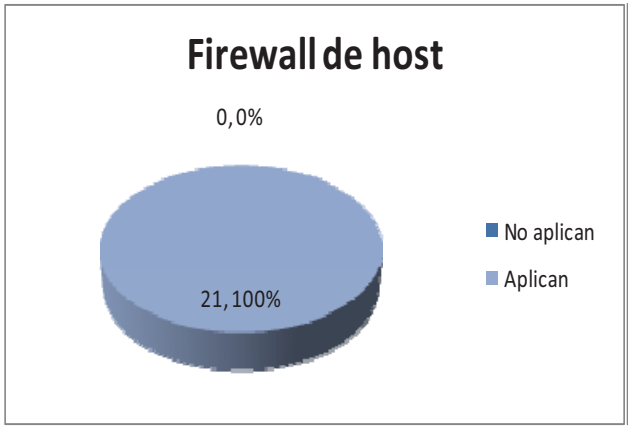

Se tienen UPS en los servidores que administra
5, 41%
7, 59%
No aplican
Aplican

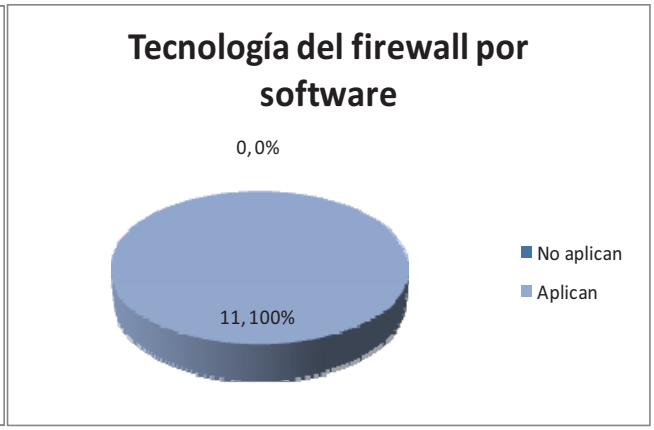

Existe un documento que contega el personal con acceso a sites vitales
2, 18%
9, 82%
No aplican
Aplican

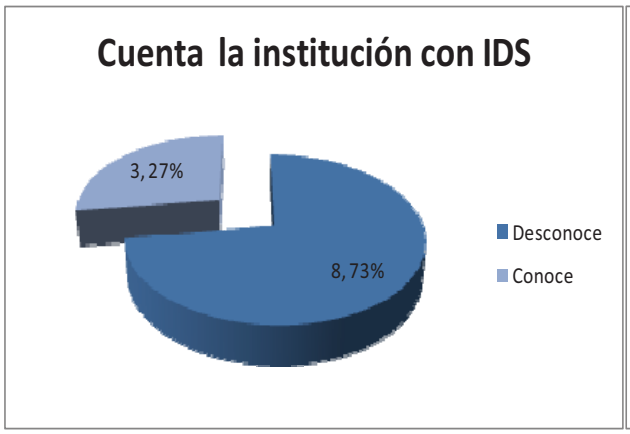

Cables de datos y eléctricos protegidos contra daños
5, 45%
6, 55%
No aplican
Aplican

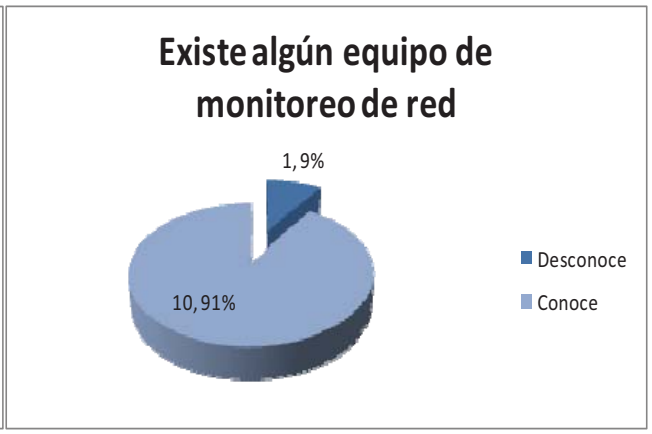

Procedimiento de control de cambios en sistemas de información
1, 9%
10, 91%
No aplican
Aplican

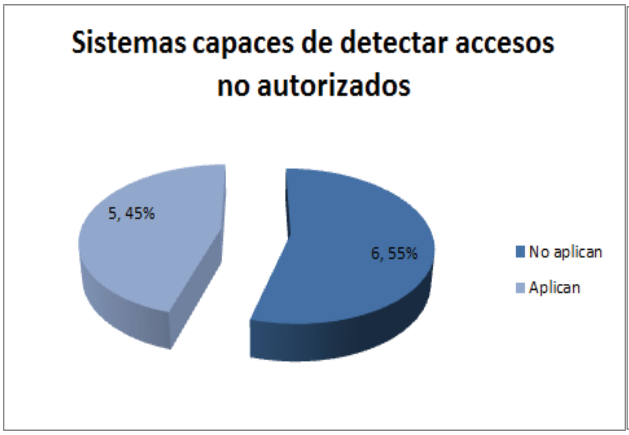

Separación de ambientes de prueba, desarrollo y operación
5, 45%
6, 55%
No aplican
Aplican


Firewall de host
0, 0%
21, 100%
No aplican
Aplican

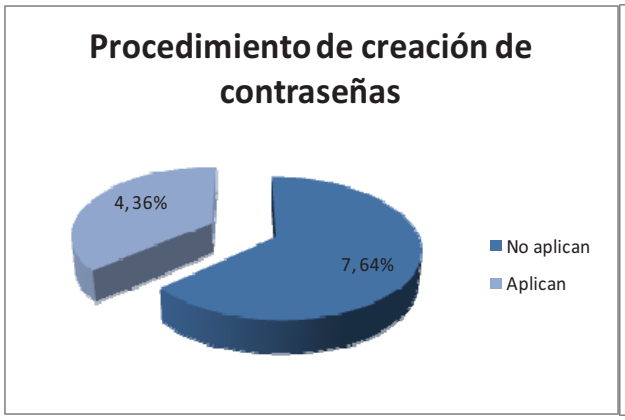

Tecnología del firewall por software
0, 0%
11, 100%
No aplican
Aplican

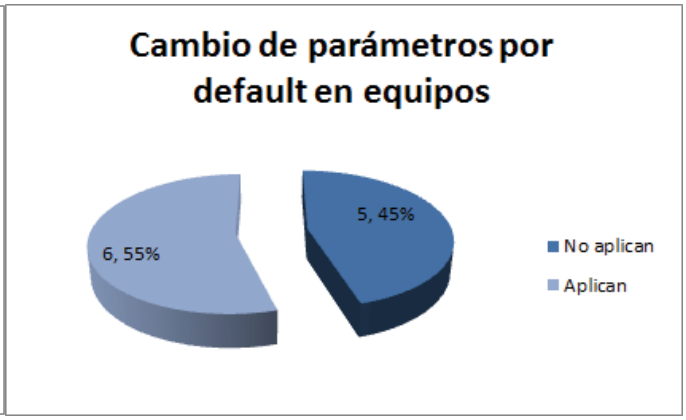

Cuenta la institución con IDS
3, 27%
8, 73%
Desconoce
Conoce


Existe algún equipo de monitoreo de red
1, 9%
10, 91%
Desconoce
Conoce

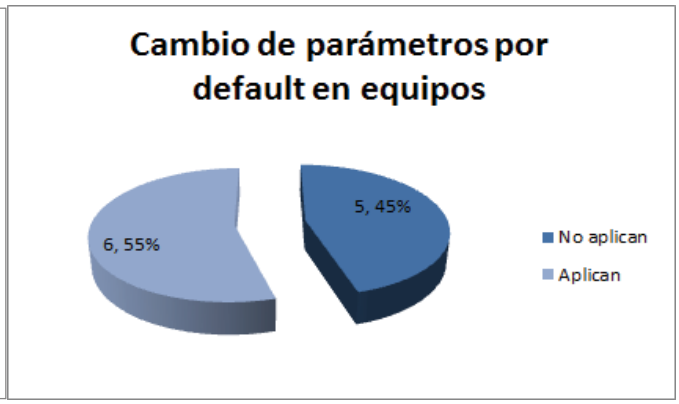

Sistemas capaces de detectar accesos no autorizados
5, 45%
6, 55%
No aplican
Aplican

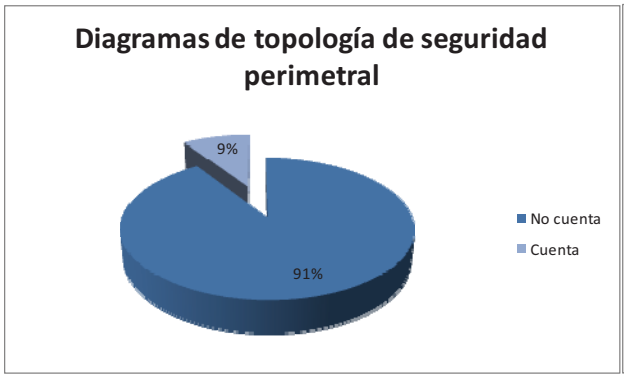

Activación de salvapantallas con contraseñas, después de cierto tiempo de inactividad
5, 45%
6, 55%
No aplican
Aplican


Procedimiento de creación de contraseñas
4,36%
7,64%
No aplican
Aplican


Cambio de parámetros por default en equipos
6, 55%
5, 45%
No aplican
Aplican

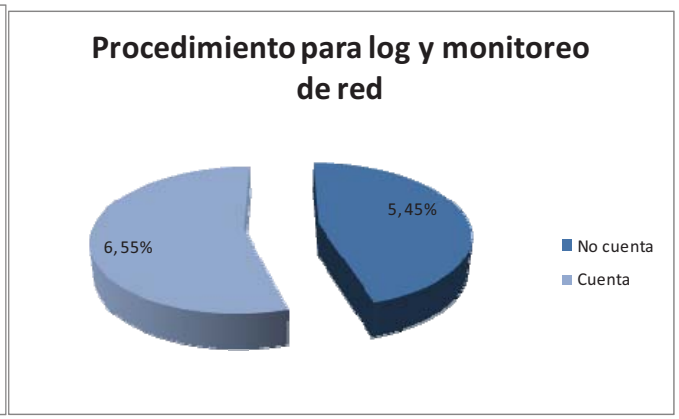

Existencia de políticas, normas y procedimientos de seguridad de la información
2
9,82%
Desconoce
Conoce


Cambio de parámetros por default en equipos
6, 55%
5, 45%
No aplican
Aplican

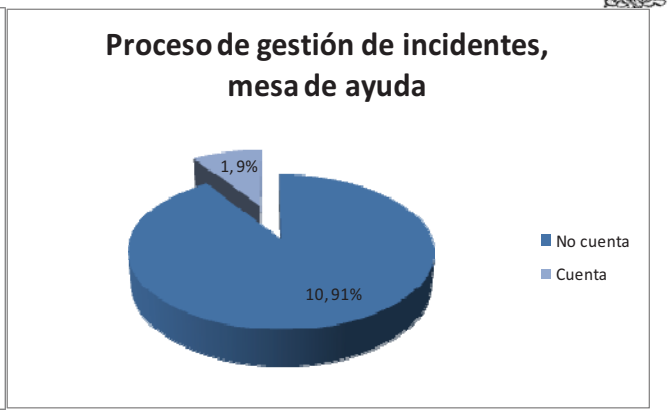

Diagramas de topología de seguridad perimetral
9%
91%
No cuenta
Cuenta

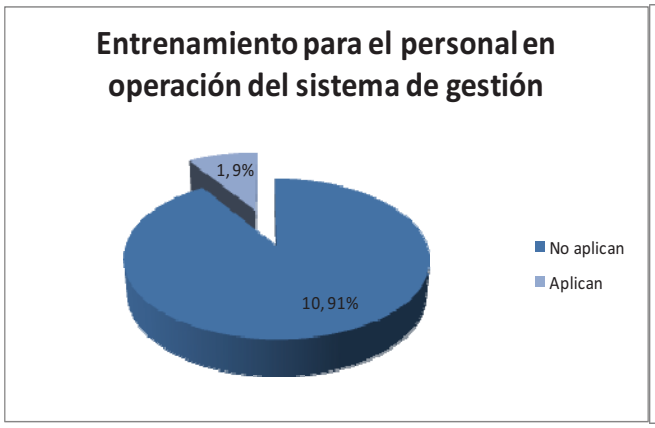

Personal entrenado para identificar y resolver incidentes
3,27%
8,73%
Desconoce
Conoce


Existe plan de continuidad, contingencia y recuperación ante desastres
2,18%
9,82%
No cuenta
Cuenta

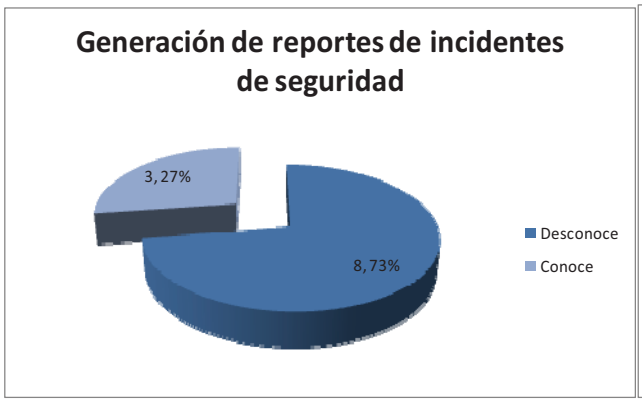

Procedimiento para log y monitoreo de red
6,55%
5,45%
No cuenta
Cuenta

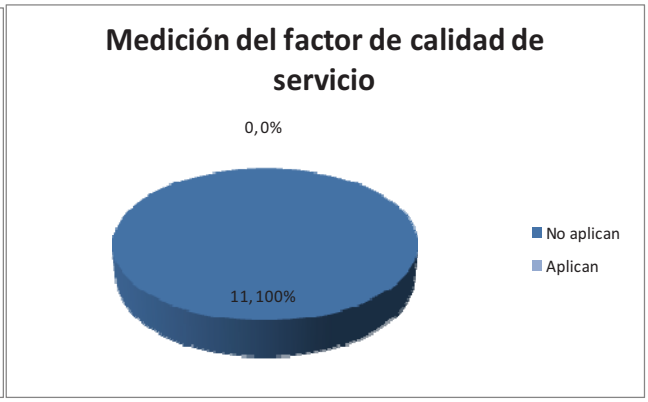

El plan de continuidad tiene contemplado aspectos de seguridad
11, 100%
0, 0%
No aplican
Aplican

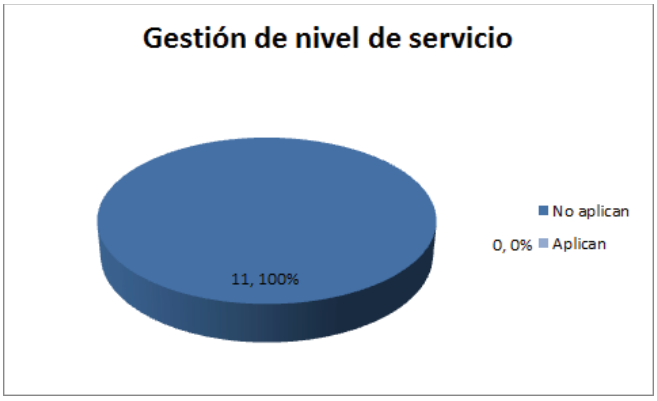

Proceso de gestión de incidentes, mesa de ayuda
1, 9%
10, 91%
No cuenta
Cuenta


Entrenamiento para el personal en operación del sistema de gestión
1, 9%
10, 91%
No aplican
Aplican

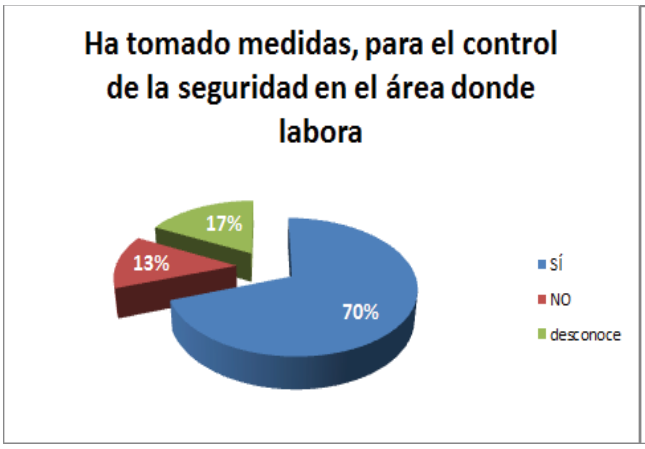

Se realiza auditoría del sistema de gestión de seguridad
No aplican
Aplican
0, 0%
11, 100%

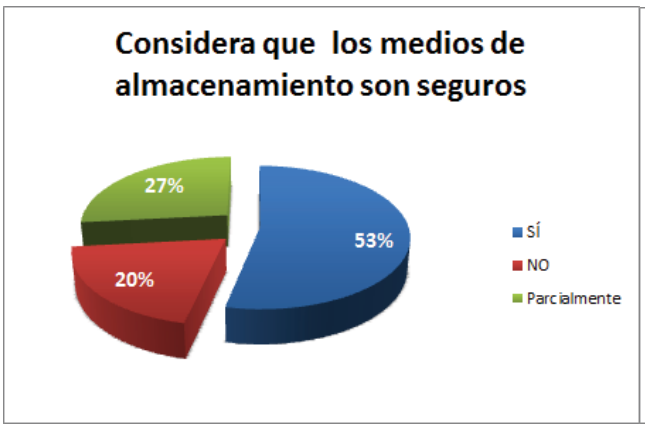

Generación de reportes de incidentes de seguridad
3, 27%
8, 73%
Desconoce
Conoce

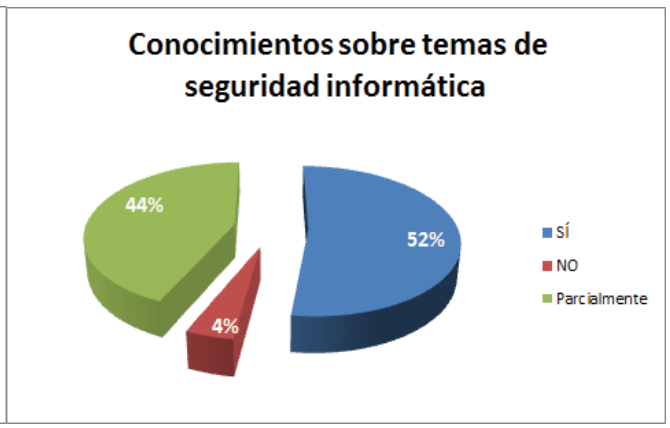

Medición del factor de calidad de servicio
0, 0%
11, 100%
No aplican
Aplican

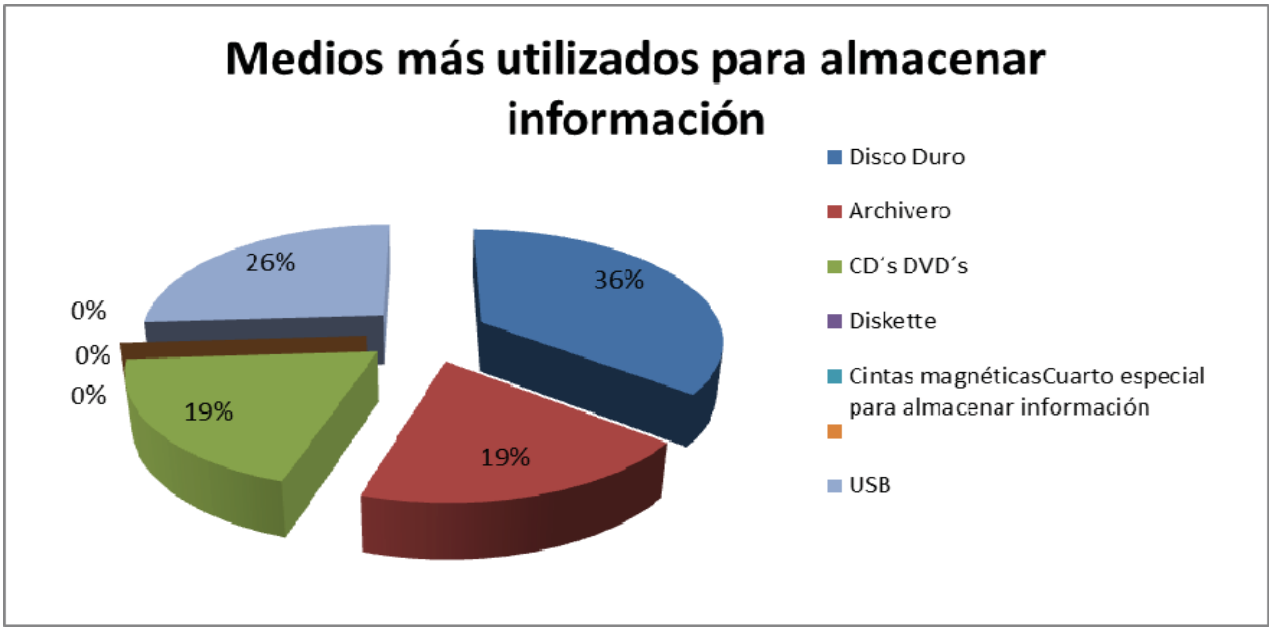

Gestión de nivel de servicio
11, 100%
No aplican
0, 0%
Aplican

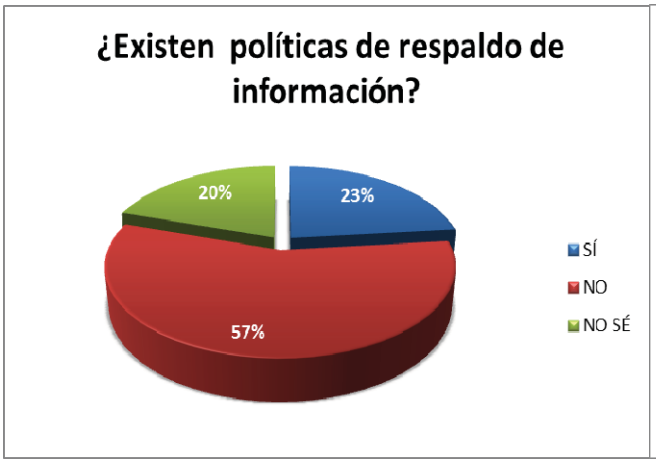
IV Resultados encuestas usuarios



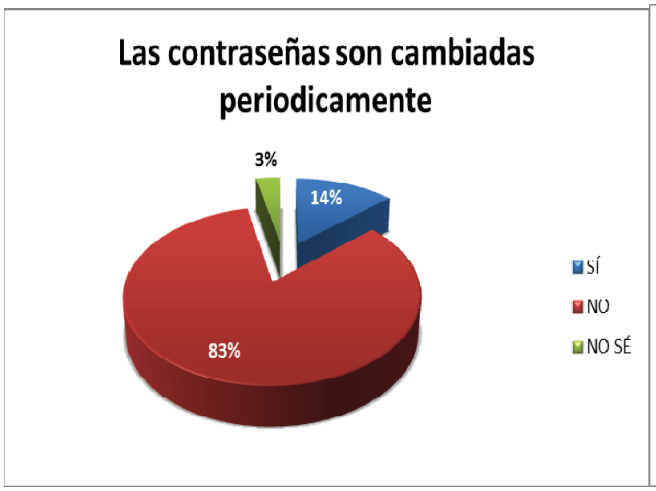


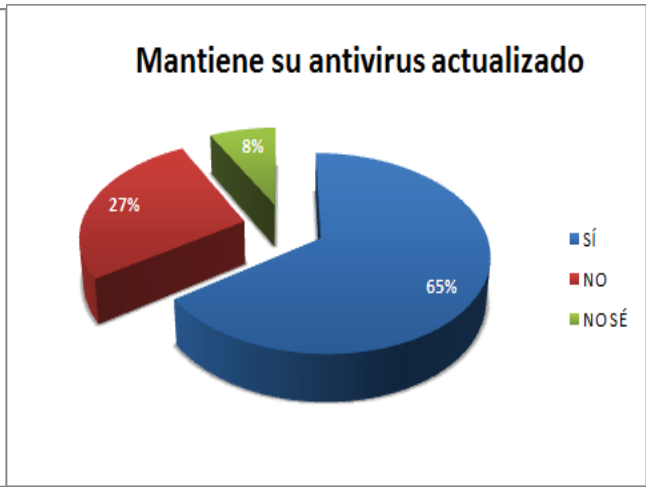




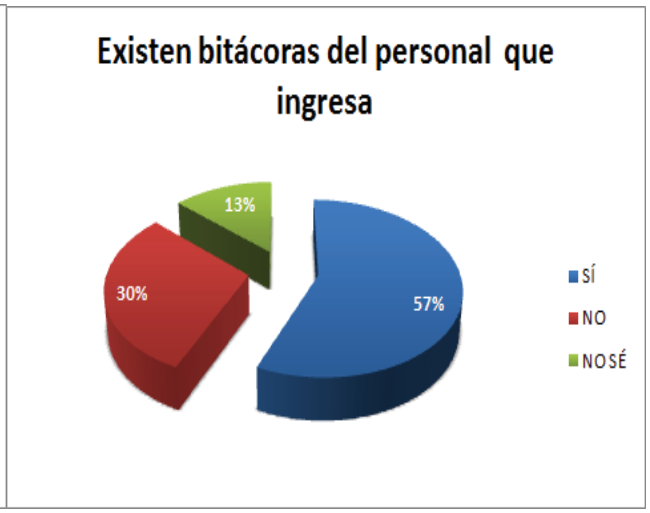

¿Existen políticas de respaldo de información?
20%
23%
57%
SÍ
NO
NO SÉ

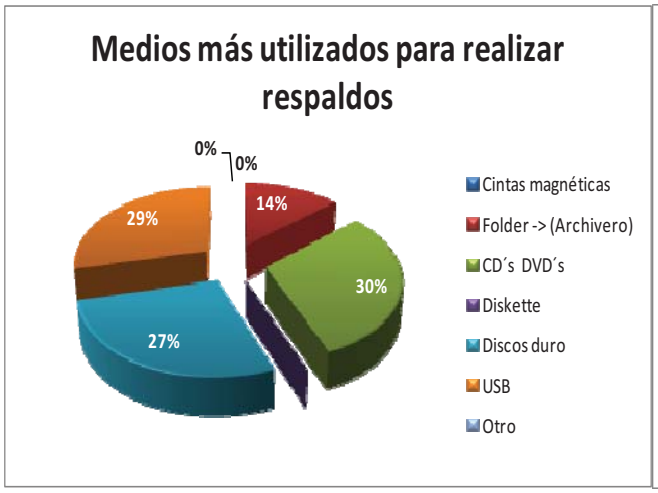

Utiliza contraseña para su equipo de cómputo
0%
30%
70%
SÍ
NO
NO SÉ

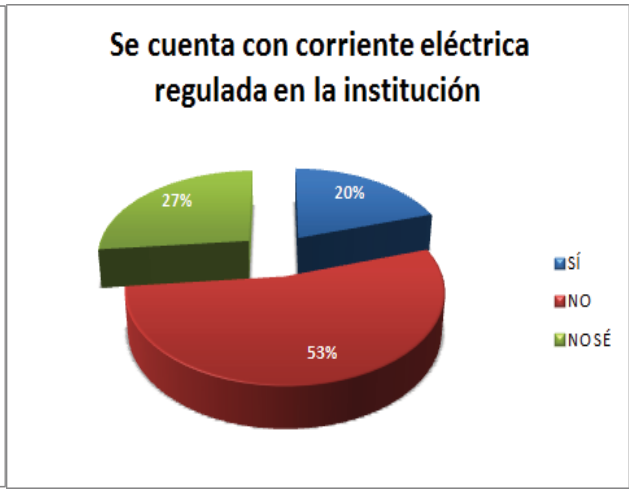

Las contraseñas son cambiadas periodicamente
3%
14%
83%
SÍ
NO
NO SÉ


Mantiene su antivirus actualizado
8%
27%
65%
SÍ
NO
NO SÉ


Se aplican las actualizaciones del sistema operativo
7%
30%
63%
SÍ
NO
NO SÉ

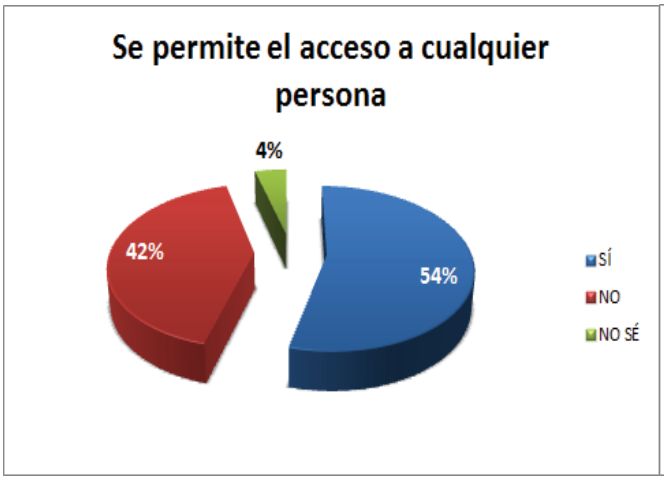

Existen bitácoras del personal que ingresa
13%
30%
57%
SÍ
NO
NO SÉ

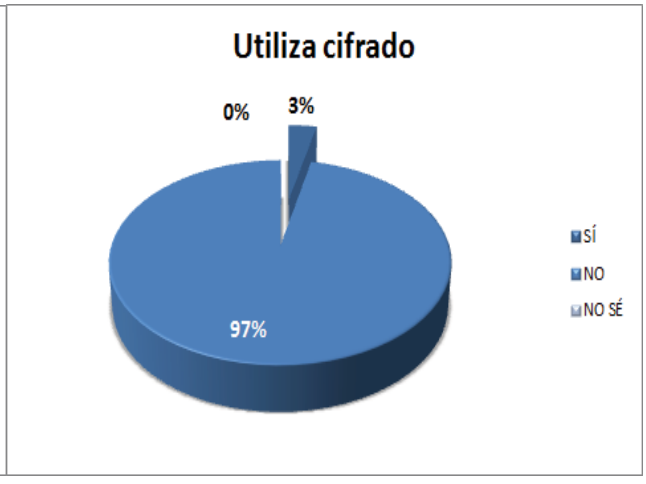

Medios más utilizados para realizar respaldos
0%
0%
14%
29%
30%
27%
Cintas magnéticas
Folder -> (Archivero)
CD´s DVD´s
Diskette
Discos duro
USB
Otro

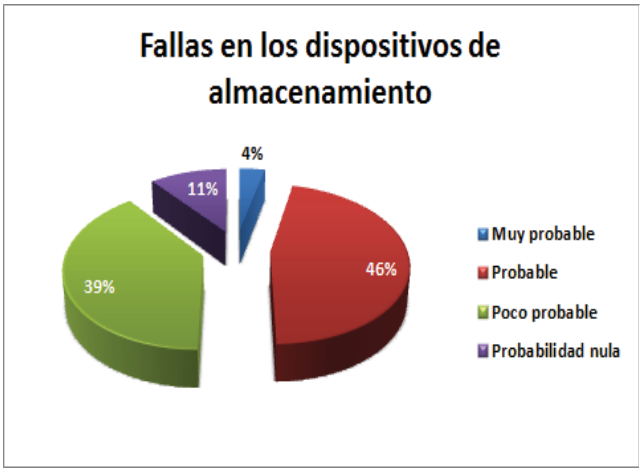

Se cuenta con corriente eléctrica regulada en la institución
27%
20%
53%
SÍ
NO
NO SÉ

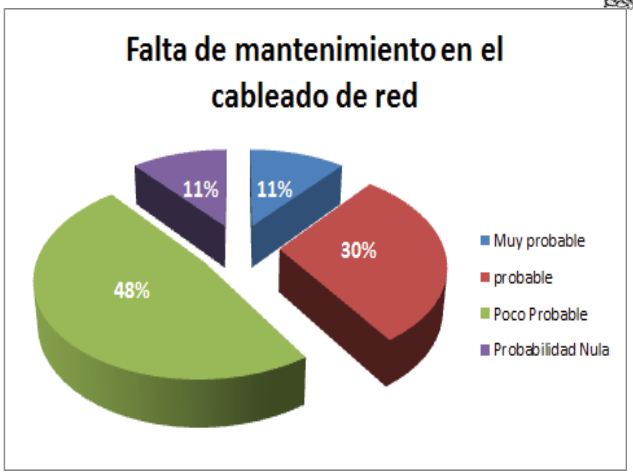

Cuenta con "no break" para el cuidado de los equipos
3%
40%
57%
SÍ
NO
NO SÉ

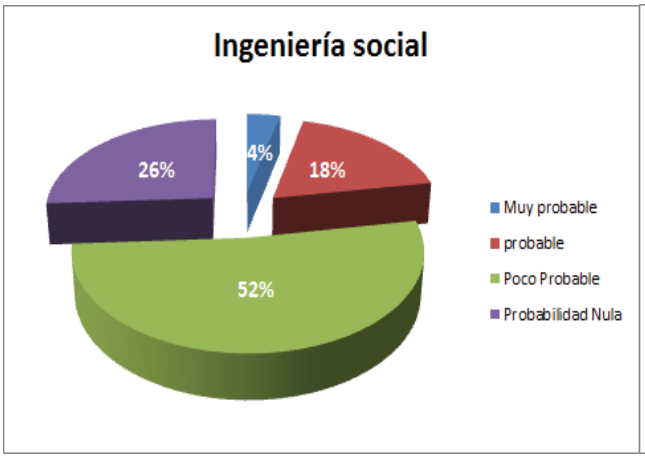

Se cuentan con extinguidores para incendio
3%
14%
83%
SÍ
NO
NO SÉ

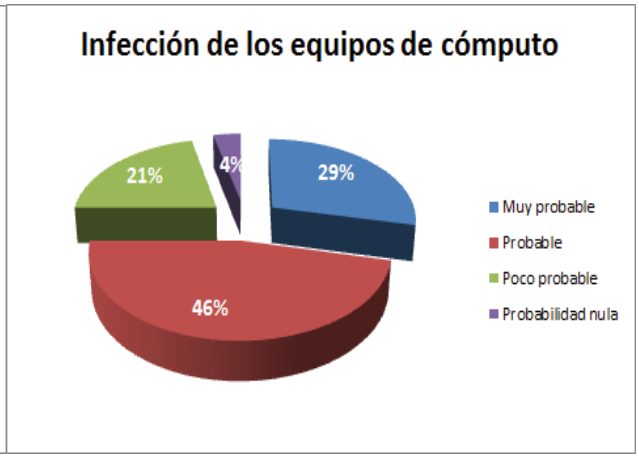

Se permite el acceso a cualquier persona
4%
42%
54%
SÍ
NO
NO SÉ

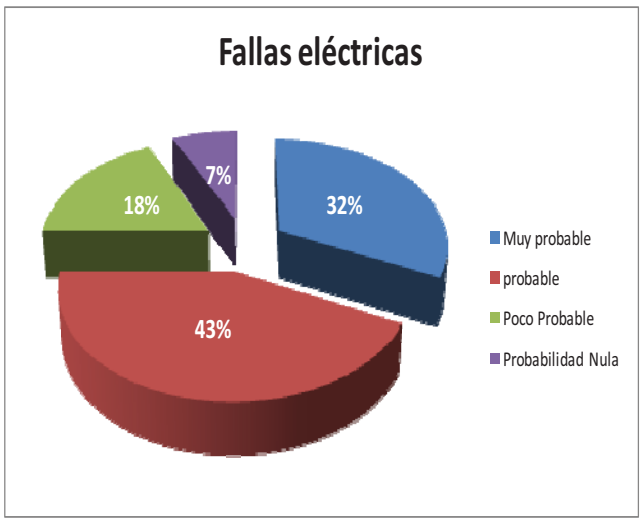

Utiliza cifrado
0%
3%
97%
SÍ
NO
NO SÉ

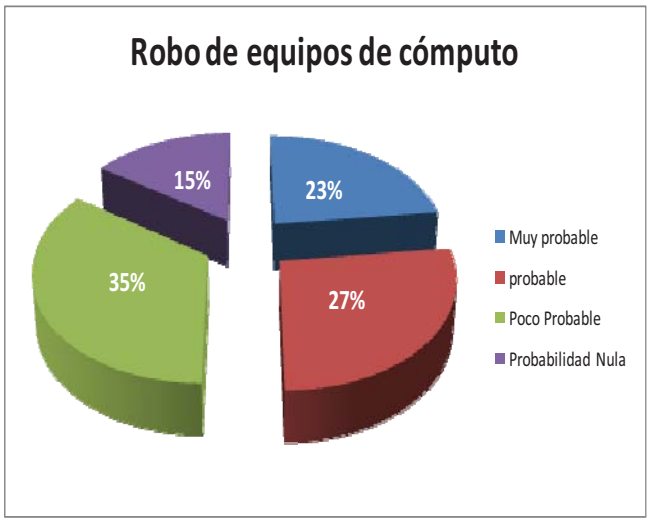

Fallas en los dispositivos de almacenamiento
4%
11%
46%
39%
Muy probable
Probable
Poco probable
Probabilidad nula

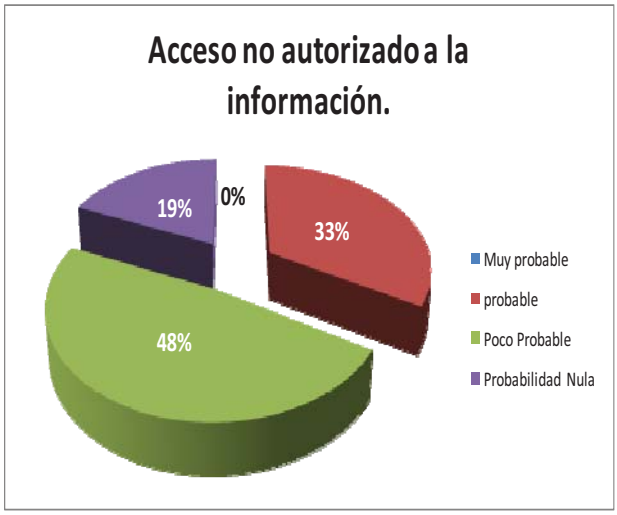

Falta de mantenimiento en el cableado de red
11%
11%
30%
48%
Muy probable
probable
Poco Probable
Probabilidad Nula

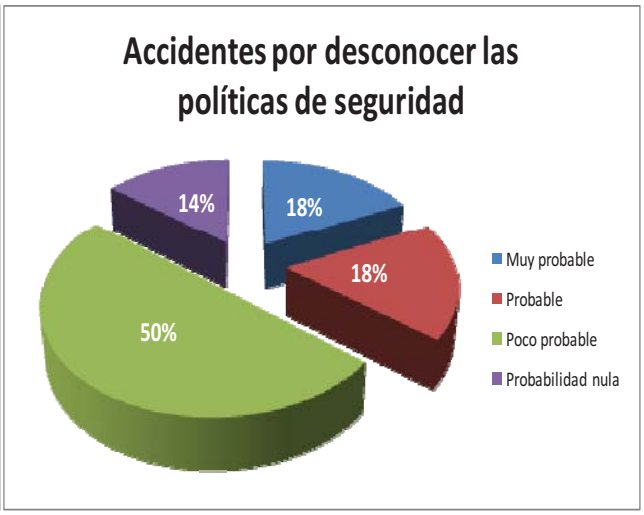

Ingeniería social
26%
4%
18%
52%
Muy probable
probable
Poco Probable
Probabilidad Nula

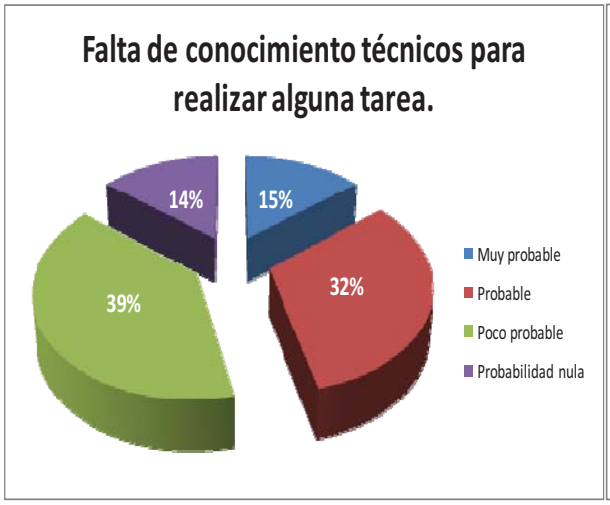

Infección de los equipos de cómputo
21%
4%
29%
46%
Muy probable
Probable
Poco probable
Probabilidad nula


Fallas eléctricas
7%
18%
32%
43%
Muy probable
probable
Poco Probable
Probabilidad Nula


Robo de equipos de cómputo
15%
23%
35%
27%
Muy probable
probable
Poco Probable
Probabilidad Nula

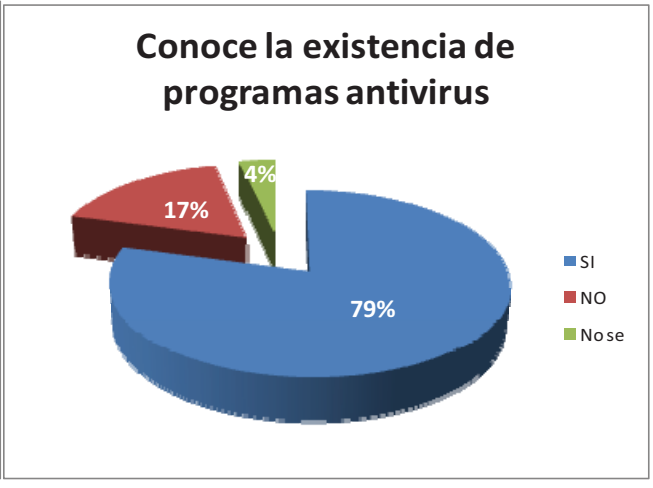

Acceso no autorizado a la información.
19%
0%
33%
48%
Muy probable
probable
Poco Probable
Probabilidad Nula

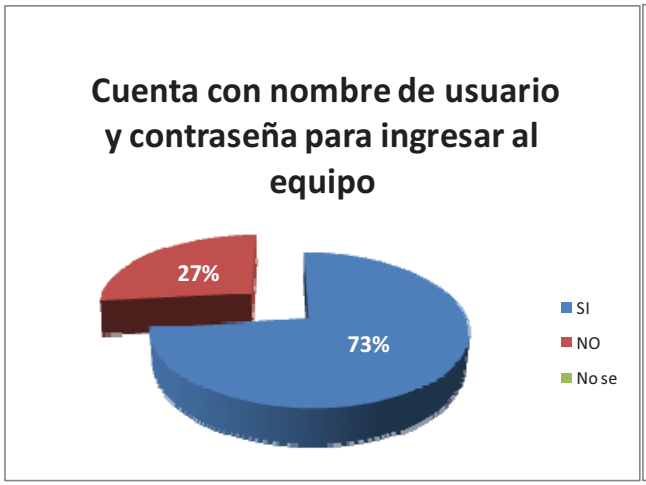

Accidentes por desconocer las políticas de seguridad
14%
18%
18%
50%
Muy probable
Probable
Poco probable
Probabilidad nula


Falta de conocimiento técnicos para realizar alguna tarea.
14%
15%
32%
39%
Muy probable
Probable
Poco probable
Probabilidad nula


Considera necesario el respaldo de información
7%
93%
Si
No


Realiza respaldo de la información que maneja
30%
0%
70%
SI
NO
No se


Conoce la existencia de programas antivirus
17%
4%
79%
SI
NO
No se


Cuenta con nombre de usuario y contraseña para ingresar al equipo
27%
73%
SI
NO
No se


Cuenta el equipo que maneja con un firewall personal:
40%
37%
23%
SI
NO
No se


Aplica las actualizaciones que se liberan para sus aplicaciones y sistema operativo
16%
13%
71%
SI
NO
No se