UNIVERSIDAD NACIONAL DEL ALTIPLANO

ESCUELA DE POSGRADO

MAESTRÍA EN INFORMATICA

TESIS

EVALUACIÓN DE SEGURIDAD EN EL SISTEMA ACADÉMICO DEL INSTITUTO SUPERIOR TECNOLÓGICO DE ACORA

PRESENTADA POR:

PEDRO FEDER PONCE CORDERO

PARA OPTAR EL GRADO ACADÉMICO DE:

MAGISTER SCIENTIAE EN INFORMÁTICA
MENCIÓN EN INGENIERÍA DE SOFTWARE

PUNO, PERÚ

2016

UNIVERSIDAD NACIONAL DEL ALTIPLANO

ESCUELA DE POSGRADO

MAESTRÍA EN INFORMÁTICA

TESIS

EVALUACIÓN DE SEGURIDAD EN EL SISTEMA ACADÉMICO DEL INSTITUTO SUPERIOR TECNOLÓGICO DE ACORA

PRESENTADA POR:

PEDRO FEDER PONCE CORDERO

PARA OPTAR EL GRADO ACADÉMICO DE:

MAGISTER SCIENTIAE EN INFORMÁTICA
MENCIÓN EN INGENIERÍA DE SOFTWARE

APROBADA POR EL SIGUIENTE JURADO:

PRESIDENTE

.....
Dr. BERNABÉ CANQUI FLORES

PRIMER MIEMBRO

.....
M. Sc. CHARLES IGNACIO MENDOZA MOLLOCONDO

SEGUNDO MIEMBRO

.....
Mg. ELMER COYLA IDME

ASESOR DE TESIS

.....
M. Sc. EDGAR HOLGUIN HOLGUIN

Puno, 04 de octubre de 2016

ÁREA: Testing de software.
TEMA: Evaluación de seguridad en sistema académico.

DEDICATORIA

A los estudiantes, docentes y autoridades de la IESTP Acora por posibilitar las condiciones necesarias para el desarrollo del presente trabajo de investigación.

A MIS PADRES que siempre me estimularon hacia el camino que dieron el ejemplo y no enseñaron sobre la importancia de la educación y conocimiento y que me apoyaron en el transcurrir de nuestros estudios.

AGRADECIMIENTOS

- A la Universidad Nacional del Altiplano de Puno y su programa de Posgrado por haberme formado profesionalmente.
- A los señores miembros del jurado, Dr. Bernabé Canqui Flores, M.Sc. Charles Ignacio Mendoza Mollocondo, Dr. Elmer Coyla Idme, por haberme brindado su tiempo en las orientaciones y mejoras para el desarrollo del presente trabajo.
- Al M.Sc. Edgar Holguin Holguin, mi asesor, quien me acompañó y asesoró en este trabajo y de quien guardo las mejores orientaciones respecto al campo de la investigación.
- A los estudiantes de Instituto Superior Tecnológico De Acora por haberme apoyado con su tiempo en el desarrollo de la investigación.

ÍNDICE GENERAL

Pág.

DEDICATORIA i
AGRADECIMIENTOS ii
ÍNDICE GENERAL iii
ÍNDICE DE FIGURAS viii
ÍNDICE DE ANEXOS xi
RESUMEN xii
ABSTRACT xiii
INTRODUCCIÓN 1

CAPÍTULO I

REVISIÓN DE LITERATURA

1.1 Sustento teórico 1
1.1.1 Sistema educativo o académico 1
1.1.2 Seguridad de la Información 2
1.2 Definición de Terminos 5
1.2.1 Active X 5
1.2.2 ADSL 5
1.2.3 Amenaza 5
1.2.4 Antivirus 6
1.2.5 Archivo de Proceso por Lotes (.bat o batch) 6
1.2.6 Archivo, Documento 6
1.2.7 Ataque 6
1.2.8 Ataque Activo 6
1.2.9 Ataque Pasivo 7
1.2.10 Auditoría 7
1.2.11 Autenticidad 7
1.2.12 Bases de datos 7
1.2.13 BIOS 7
1.2.14 Carpeta 8
1.2.15 Chat 8
1.2.16 COBOL 8
1.2.17 Cookie 8

1.2.18 CPD 8
1.2.19 Criptografía 8
1.2.20 Datos 9
1.2.21 Departamento de cómputo 9
1.2.22 Dominio 9
1.2.23 DOS (MS/DOS) 9
1.2.24 Equipo de cómputo 9
1.2.25 Equipo de telecomunicaciones 10
1.2.26 Filtro de paquetes 10
1.2.27 Finger 10
1.2.28 Firewall 10
1.2.29 Firma digital 10
1.2.30 FTP 11
1.2.31 Gusano 11
1.2.32 Hacker 11
1.2.33 Host 11
1.2.34 HTML 11
1.2.35 HTTP 11
1.2.36 Hub 11
1.2.37 Identificación 12
1.2.38 Incidente 12
1.2.39 Infección 12
1.2.40 Integridad 12
1.2.41 Intranet 13
1.2.42 IP Address 13
1.2.43 ISP 13
1.2.44 Local Area Network 13
1.2.45 Macro / Virus de Macro 13
1.2.46 MAN 13
1.2.47 Mensaje de datos 14
1.2.48 NAT 14
1.2.49 Navegador 14
1.2.50 POP 14
1.2.51 Privacidad 14

1.2.52 Programas (archivos .exe y .com) 14
1.2.53 Protocolo 15
1.2.54 Redireccionar 15
1.2.55 Router 15
1.2.56 SATAN 15
1.2.57 Script 15
1.2.58 Seguridad 15
1.2.59 Sendmail 16
1.2.60 SHTTP 16
1.2.61 Sistema Operativo (S.O.) 16
1.2.62 SMTP 16
1.2.63 Spam 17
1.2.64 SSL 17
1.2.65 TCP 17
1.2.66 Telnet 17
1.2.67 Texto Plano 17
1.2.68 Trojan Horse 17
1.2.69 URL 17
1.2.70 WAN 17
1.2.71 Webmin 18
1.2.72 WWW 18
1.3 Antecedentes 18

CAPÍTULO II

PLANTEAMIENTO DEL PROBLEMA

2.1 Planteamiento de la investigación 22
2.2 Objetivos 23
2.2.1 Objetivo general 23
2.2.2 Objetivos específicos 23

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1 Tipo del problema de investigación 24
3.2 Población de la investigación 24
3.3 Muestra de la investigación 24
3.4 Ubicación y descripción de la población o ámbito de estudio 25

3.5 Técnicas e instrumentos para recolectar información 25
3.5.1 Encuestas 26
3.5.2 Entrevistas. 26
3.5.3 Análisis documental 26

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1 Informe de relevamiento 28
4.1.1 Seguridad lógica. 28
4.1.1.1 Identificación de usuarios 28
4.1.1.2 Autenticación 56
4.1.1.3 Passwords 58
4.1.2 Seguridad en las comunicaciones 58
4.1.2.1 Topología de red 59
4.1.2.2 Conexiones externas 62
4.1.2.3 Configuración lógica de la red 65
4.1.2.4 Antivirus 66
4.1.3 Seguridad de las aplicaciones 67
4.1.3.1 Software 67
4.1.3.2 Seguridad de base de datos 68
4.1.3.3 Control de aplicaciones en Psc 68
4.1.4 Seguridad física 69
4.1.4.1 Equipamiento 69
4.1.4.2 Control de acceso físico a los centros de computo 70
4.1.4.3 Control de acceso a equipos 71
4.1.4.4 Dispositivos de soporte 72
4.1.4.5 Estructura del edificio 72
4.1.4.6 Cableado estructurado 73
4.1.5 Auditorias y revisiones 74
4.1.5.1 Chequeos del sistema 74
4.1.5.2 Responsabilidad del encargado de seguridad 74
4.1.5.3 Auditoria de control de acceso 75
4.2 Informe de debilidades y recomendaciones 76
4.2.1 Seguridad lógica 76
4.2.1.1 Identificación de usuarios 76

4.2.1.2 Passwords 77
4.2.2 Seguridad en las comunicaciones 77
4.2.2.1 Topología de la red y conexiones externas 77
4.2.2.2 Configuración lógica de la red 78
4.2.2.3 Antivirus 78
4.2.3 Seguridad de base de datos 78
4.2.3.1 Seguridad de base de datos 78
4.2.3.2 Control de aplicaciones de Pcs 79
4.2.4 Seguridad física 79
4.2.4.1 Control de acceso físico a los centros de computo 79
4.2.4.2 Dispositivo de soporte 80
4.2.4.3 Estructura del edificio 80
4.2.4.4 Cableado estructurado 80
4.2.5 Auditorias y revisiones 81
4.2.5.1 Chequeos del sistema 81
4.2.5.2 Responsabilidades del encargado de seguridad 81
4.2.5.3 Auditoria de control de acceso 81
CONCLUSIONES 82
RECOMENDACIONES 83
BIBLIOGRAFÍA 85
ANEXOS 89

ÍNDICE DE FIGURAS

Pág.

1. Generación de accesos docente módulo de secretaria académica 29
2. Login para alta de docentes 29
3. Ingreso de datos laborales del docente 30
4. Ingreso de datos personales del docente 31
5. Ingreso de datos de acceso 31
6. Asignación de cargos administrativos 32
7. Modo de cambiar cargo administrativo 32
8. Vínculo laboral con la institución 33
9. Ejemplo de reporte en formato PDF. 33
10. Formato Excel 34
11. Módulo para dar de alta a los usuarios alumnos en masa 34
12. Generación de accesos alumnos, módulo de secretaria académica 35
13. Login para el acceso generado, registró de nuevo alumno 35
14. Registro de datos académicos del alumno 36
15. Registro de datos personales el alumno 37
16. Entorno de ingreso al sistema por módulos 38
17. Login Usuario Secretario académico 40
18. Matricula de alumnos 40
19. Elección de un alumno para su matricula 41
20. Administrar exámenes de recuperación 41
21. Formulario para reportar ranking 41
22. Reporte de Ranking 42
23. Formulario para obtener el record académico 42
24. Reporte de record académico 42
25. Formulario para reportar nóminas de matrícula 43
26. Reporte de nóminas de matrícula 43
27. Formulario para reportar acta consolidada 43
28. Reporte de acta consolidada 44
29. Reporte de actas adicionales de recuperación 44
30. Reporte de actas adicionales de recuperación 44
31. Reporte de actas adicionales de repitencia 45

32. Reporte de actas adicionales de repitencia 45
33. Formulario de búsqueda de alumno 45
34. Reporte de boleta de información individual 46
35. Formulario para el reporte de boleta de información grupal 46
36. Reporte de boleta de información grupal 46
37. Generación e impresión de accesos alumnos 47
38. Generación e impresión de accesos docentes 47
39. Configuración de la institución 47
40. Actualización de datos de la institución 48
41. Administración de resoluciones 48
42. Administrar cargos administrativos 48
43. Cambiar un cargos administrativo 48
44. Relación de docentes 49
45. Vista preliminar de impresión de docentes 49
46. Administración del vínculo laboral 49
47. Formulario para actualizar datos del docente 50
48. Formulario para cambiar contraseña del docente 50
49. Listado de alumnos por unidad académica 50
50. Listado de alumnos exportado a formato Excel 51
51. Listado de unidades académicas para llenado de notas 51
52. Llenado de notas 51
53. Listado de unidades académicas para realizar reportes 52
54. Reporte generado por el docente 52
55. Distribución de carga académica 52
56. Reporte PDF de la distribución de la carga académica 53
57. Creación de horario según semestre turno y sección 53
58. Reporte PDF del horario creado 53
59. Asignamiento de jurados para recuperación 54
60. Reporte PDF del acata de evaluación de recuperación 54
61. Publicación de recuperaciones 54
62. Asignación de unidades académicas opcionales 54
63. Visualización programación académica 55
64. Visualización de horarios 55
65. Visualización de notas 55

66. Cambio de contraseña 56
67. *Actualización de datos* 56
68. Pantalla de login 56
69. Login para el proveedor del sistema 57
70. Alumnos en el centro de Cómputo 01 59
71. Centro de cómputo 02 – panorámico 60
72. Centro de computo 02 60
73. Alumnos conectándose al Interne WIFI 61
74. Alumnos conectados a la red WIFI fuera de los salones de clase 61
75. Switch conectado con UTP 62
76. Servidor de la institución 63
77. Grafico Topológico De La Red 64
78. Instituto de Educación Superior Tecnológico Publico Acora 73

ÍNDICE DE ANEXOS

		Pág.
1.	Relevamiento inicial	90
2.	Seguridad lógica	92
3.	Seguridad en las comunicaciones	101
4.	Seguridad de las aplicaciones	114
5.	Seguridad física	120
6.	Administración del centro de cómputos	127
7.	Auditorías y revisiones	131
8.	Plan de contingencias	141

RESUMEN

El El presente trabajo de tesis, titulado “Evaluación de Seguridad en el Sistema Académico del Instituto Superior Tecnológico de Acora”, se realizó con el objetivo de evaluar el sistema académico del Instituto de Educación Superior Tecnológico de Acora, considerando la tecnología aplicada para evaluar la seguridad de la información en dicha institución. La metodología utilizada en el desarrollo del presente trabajo de investigación se basa, en su primera parte, en el desarrollo del informe de relevamiento donde se observa cómo se llevan a cabo los distintos procesos y las tecnologías con la que cuenta la institución, en este informe se tocan los aspectos de la seguridad lógica, seguridad en las comunicaciones, seguridad en las aplicaciones, seguridad física, auditorias y revisiones. En cuanto a la segunda parte se realiza el informe de debilidades y recomendaciones para lo cual ejecutamos el proceso de identificación de debilidades y defectos, para luego continuar con las recomendaciones, considerando previamente el análisis realizado en el primer apartado. En cuanto a la normatividad utilizamos los estándares y guías de COBIT (Control Objetive for Informatión Technology), ISO 17799 (British Standard 7799), ISACA (Information Systems Audit and Control Association).

Palabras clave: COBIT, evaluación, Internet, ISO, seguridad y sistema académico..

ABSTRACT

This thesis work, entitled "Assessment of Security in the Academic System of the Higher Institute of Technology of Acora", was conducted with aim on evaluating the academic system of the Technological Institute of Higher Education of Acora, considering the technology applied to assess safety of the information in said institution. The methodology used in the development of this research work is based, in its first part, on the development of the survey report, which shows how the different processes and technologies are carried out by the institution, in this report the aspects of logical security, security in communications, security in applications, physical security, audits and revisions are touched upon. In the the second part, the report of weaknesses and recommendations is made, for which we execute the process of identification of weaknesses and defects, and then continue with the recommendations, previously considering the analysis made in the first part. Regarding the regulations, we use the standards and guides of COBIT (Control Objective for Information Technology), ISO 17799 (British Standard 7799), and ISACA (Information Systems Audit and Control Association)

Keywords: Academic system, COBIT, evaluation, internet, ISO and Security.

INTRODUCCIÓN

El Ministerio de Educación del Perú (MINEDU), es el órgano superior en el sector educación a nivel nacional, teniendo como misión "Garantizar derechos, asegurar servicios educativos de calidad y promover oportunidades deportivas a la población para que todos puedan alcanzar su potencial y contribuir al desarrollo de manera descentralizada, democrática, transparente y en función a resultados desde enfoques de equidad e interculturalidad." (http://www.minedu.gob.pe/p/ministerio-mision-vision.html), en tal sentido es responsable de las actividades académicas y del aprendizaje en los distintos niveles de educación, desde el nivel inicial hasta la educación superior tecnológica, pedagógica, escuelas de formación artística (ESFA) y los centros de estudio técnico productivos (CETPRO), promoviendo la interculturalidad de nuestra nación, promoviendo la formación de personas responsables con la sociedad comprometiéndolos con el desarrollo social.

La Dirección Regional de Educación - Puno (DREP), es el órgano superior de educación en el departamento de Puno, cuya misión es "Al 2015 la Región Puno, desarrolla con una educación integral de calidad, humanista, científica, tecnológica, inclusiva, democrática, descentralizada e innovadora, identificada con las culturas andinas y la conservación del ecosistema a través de la participación activa de autoridades regionales, locales y sociedad civil como miembros de una comunidad educadora y ética, que propicie espacios de interacción multisectorial; con docentes éticos, creativos, investigadores y capaces de adaptarse a los cambios y los nuevos escenarios, respetando las prácticas interculturales e idiomas originarios, comprometidos con la cultura de paz, para el desarrollo humano y productivo de la región. Los estudiantes se desempeñan con eficiencia y eficacia en la vida y el mundo laboral, practicando valores; capaces de enfrentar los retos de la globalización y liderar el desarrollo productivo y empresarial, en una sociedad democrática, justa y solidaria." (http://www.drepuno.gob.pe/web/2011-11-17-17-25-11/mision-y-vision.html), es la entidad responsable de formar jóvenes responsables con la sociedad, conscientes de la problemática regional y recibiendo una formación integral es la responsable por la educación integral del departamento de Puno.

La Educación Superior Tecnológica es representada ante la DREP mediante el especialista de la Educación Tecnológica el cual es responsable por velar que todos los Institutos de Educación Superior Tecnológico cumplan fielmente los reglamentos, leyes

y normas que estipula el estado y el MINEDU así como también cumplan con las disposiciones legales que demanda la DREP.

Los Institutos de Educación Superior Tecnológico Públicos, están en la obligación de presentar ante la DREP y su representante el especialista de educación tecnológica los formatos de nóminas de matrículas que contiene el registro de los alumnos matriculados en la institución, este proceso se lleva a cabo cada inicio de semestre, es decir aproximadamente en el mes de abril y en el mes de setiembre de cada año, así como también están en la obligatoriedad de presentar las actas consolidadas semestrales, actas consolidadas de repitencia y actas consolidadas de recuperación, en dichas actas se tiene registrado las notas de los alumnos por unidad académica, donde se detallan la cantidad de los alumnos que fueron desaprobados con notas menores a trece y alumnos desaprobados por inasistencia (DPI) constando las firmas de los docentes que realizaron el dictado de las unidades académicas en el semestre que indica cada acta.

El Instituto de Educación Superior Tecnológico Publico – Acora (IESTP – Acora) cuenta con la oficina de Secretaría de Unidad Académica, una de las funciones más importantes que cumple esta oficina es la de presentar semestralmente la documentación anteriormente indicada ante el especialista de educación tecnológica de la DREP, siendo antes firmada por el Director de la institución y por el responsable de dicha oficina y de ser necesario por los docentes que pertenecen a la institución, es el caso de las actas consolidadas.

Actualmente el IESTP – Acora cuenta son un Sistema Académico de fecha 25 de Octubre del 2010, en el que se encuentran registrados todos los alumnos de la institución, incluyendo a aquellos que comenzaron un semestre y dejaron de estudiar en un momento determinado, también se encuentra registrado todas las notas de los alumnos que están estudiando en la institución desde el segundo semestre del año 2010 (2010 - II).

Actualmente el Sistema Académico sigue siendo usado por la oficina de secretaría académica, mostrando algunas fallas por falta de mantenimiento físico de la computadora donde se tiene instalado el Sistema Académico y fundamentalmente a causa el ciclo de vida del software.

CAPÍTULO I

REVISIÓN DE LITERATURA

1.1 Sustento teórico

1.1.1 Sistema educativo o académico

El sistema académico es una herramienta que puede ser aplicada en centros de enseñanza como: institutos, escuelas, colegios, academias, universidades, etc.

Un sistema educativo, de este modo, es una estructura formada por diversos componentes que permiten educar a la población. Las escuelas, las universidades, las bibliotecas y los docentes, entre otros, forman parte de este sistema.

La principal ventaja del sistema es la organizacion, administración , además sirve como fuente de datos para toda la institución educativa, ya que se establecen roles de trabajo para cada usuario que tiene acceso al sistema. Modernizando de esta forma los procesos académicos de los alumnos y de la institución. (Echeverria, 2018)

El Sistema Academico puede realizar:

- Administrar y controlar mejor la información de docentes y alumnos
- Crear y asignar niveles académicos (grados o niveles de bachillerato) asignado un docente como coordinador
- Crear las diferentes asignaturas y asignar el respectivo docente que la impartirá junto con los grados donde la impartirá

- Crear los diferentes periodos o áreas de evaluación asignado los porcentajes respectivos de cada periodo o área
- Crear las diferentes evaluaciones y porcentajes de cada periodo o área
- Imprimir colectores vacíos por asignatura para el procesamiento de notas
- Ingreso de notas al sistema por parte del docente que imparte la asignatura o por parte de departamento académico
- Escribir comentarios por alumno sobre su conducta o los resultados académicos obtenidos durante el periodo para ser utilizado por el coordinador.
- Impresión de formularios como nuevo ingreso, etc.
- Generar constancia de notas por alumno
- Crear e imprimir las boletas de nota por alumno o por grado
- Entre otras tareas...

1.1.2 Seguridad de la Información

La seguridad de la información es un conjunto de medidas preventivas de1 las organizaciones y de los sistemas de infromacion que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial. Este campo ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital y administración de sistemas de gestión de seguridad, entre otros. (Matalobos, 2009)

El acceso a cierta información se clasifica como:

- **Crítica:** Es indispensable para la operación de la empresa.
- **Valiosa:** Es un activo de la empresa y muy valioso.
- **Sensible:** Debe de ser conocida por las personas autorizadas

a) Confidencialidad

La confidencialidad es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.

b) Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) Grosso modo, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

La integridad también es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada, para salvaguardar la precisión y completitud de los recursos.

La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra datos importantes que son parte de la información.

La integridad garantiza que los datos permanezcan inalterados excepto cuando sean modificados por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital es uno de los pilares fundamentales de la seguridad de la información.

c) Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La alta disponibilidad sistemas objetivo debe estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

Garantizar la disponibilidad implica también la prevención de ataque de denegación de servicio. Para poder manejar con mayor facilidad la seguridad de la información, las empresas o negocios se pueden ayudar con un sistema de gestión que permita conocer, administrar y minimizar los posibles riesgos que atenten contra la seguridad de la información del negocio.

La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos

para cumplir con los niveles de servicio que se requiera. Tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web etc, mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

d) Autenticación o autentificación

Es la propiedad que permite identificar el generador de la información. Por ejemplo al recibir un mensaje de alguien, estar seguro que es de ese alguien el que lo ha mandado, y no una tercera persona haciéndose pasar por la otra (suplantación de identidad). En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y contraseñas de acceso.

Esta propiedad se puede considerar como un aspecto de la integridad -si está firmado por alguien, está realmente enviado por el mismo- y así figura en la literatura anglosajona.

1.2 Definición de Terminos

1.2.1 Active X

Es un lenguaje de programación apoyado en controles OLE, Visual Basic y librerías del entorno Windows (OCX) de Microsoft. Active X permite que interactúen aplicaciones Windows con el World Wide Web. (Cabarcas Gómez, 2013)

1.2.2 ADSL

(Asymmetric Digital Suscribe Line - Línea de Usuario Digital Asimétrica). Usa la infraestructura telefónica actual para proveer servicios de transmisión de datos en alta velocidad. (Gotzy, 2017)

1.2.3 Amenaza

Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal o equipo informático, o causar la difusión no autorizada de

información confiada a una computadora. Ejemplo: fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados. (Victdelr, 2013).

1.2.4 Antivirus

Son todos aquellos programas que permiten analizar memoria, archivos y unidades de disco en busca de virus. Una vez que el antivirus ha detectado alguno de ellos, informa al usuario procediendo inmediatamente y de forma automática a desinfectar los ficheros, directorios, o discos que hayan sido víctimas del virus. (Gotzy, 2017)

1.2.5 Archivo de Proceso por Lotes (.bat o batch)

Los ficheros de proceso por lotes o ficheros Batch se caracterizan por tener extensión BAT. Son ficheros de texto que contienen comandos, uno por cada línea escrita. Cuando se ejecuta este tipo de ficheros, cada una de las líneas en él escritas se va ejecutando de forma secuencial. (Leyes, 2018)

1.2.6 Archivo, Documento

Estos términos tienen el mismo significado y hacen referencia a la información que se encuentra en un soporte de almacenamiento informático. Es el trabajo real que realiza cada usuario (textos, imágenes, bases de datos, hojas de cálculo, etc.). Cada uno de ellos se caracteriza por tener un nombre identificativo. El nombre puede estar seguido de un punto y una extensión, compuesta por tres caracteres que identifican el tipo de fichero del que se trata. Algunas extensiones comunes son: EXE y COM (ficheros ejecutables, programas), TXT y DOC (ficheros de texto), etc.

1.2.7 Ataque

Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora. (UCB, 2005)

1.2.8 Ataque Activo

Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado

información confiada a una computadora personal. Ejemplo: borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora. (Victdelr, 2013)

1.2.9 Ataque Pasivo

Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene. (Gobiernodigital, 2018)

1.2.10 Auditoría

Llevar a cabo una inspección y examen independiente de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y procedimientos operativos, y para recomendar cualquier cambio que se estime necesario.

1.2.11 Autenticidad

Capacidad de determinar si una lista de personas ha establecido su reconocimiento y/o compromiso sobre el contenido del documento electrónico.

1.2.12 Bases de datos

Es un conjunto de datos interrelacionados y un conjunto de programas para accesarlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápido.

1.2.13 BIOS

Es la abreviatura de Basic Input / Output System e identifica al software o conjunto de programas que arrancan el ordenador (antes de encontrarse un disco de sistema) cuando se pulsa el botón de encendido. La BIOS es un programa que se no se encuentra en la memoria RAM (Random Access Memory – memoria de acceso aleatorio) pues al apagar el ordenador se borraría, sino en la memoria

principal o ROM (Read Only Memory -Memoria de Sólo Lectura), cuyo almacenamiento es permanente. (Gotzy, 2017).

1.2.14 Carpeta

Se trata de divisiones (no físicas sino lógicas) en cualquier tipo de disco donde son almacenamos determinados ficheros. Forman parte de una manera de organizar la información del disco, guardando los documentos como si de una carpeta clasificadora se tratase. (Rootsecure, 2008)

1.2.15 Chat

Se trata de conversaciones escritas en Internet. Mediante una conexión a la red y un programa especial, es posible conversar (mediante texto escrito) con un conjunto ilimitado de personas, al mismo tiempo. (Rootsecure, 2008)

1.2.16 COBOL

(Common Organization Business Oriented Language) lenguaje de programación creado en la década del 60. Confidencialidad: capacidad de mantener datos inaccesibles a todos, excepto a una lista determinada de personas. (Gotzy, 2017)

1.2.17 Cookie

Procedimiento ejecutado por el servidor que consiste en guardar información acerca del cliente para su posterior recuperación En la práctica la información es proporcionada desde el visualizador al servidor del Word Wide Web vía una forma o un método interactivo que puede ser recuperado nuevamente cuando se accede al servidor en el futuro. Es utilizado por ejemplo para el registro a un servicio. (Matpec, 2018)

1.2.18 CPD

Centro de procesamiento de datos, centro de cómputos.

1.2.19 Criptografía

(Encriptación) es la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original.

1.2.20 Datos

Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc. (Chanamé, 2015)

1.2.21 Departamento de cómputo

Es la entidad encargada del buen uso de las tecnologías de la computación, organización y optimización de los recursos computacionales de la institución. Es la entidad encargada de desarrollar el plan estratégico que favorezca la prestación de servicios eficientes, eficaces y de utilidad en la transmisión de datos para apoyar efectivamente los requerimientos del usuario. Es la entidad encargada de ofrecer sistemas de información administrativa integral permitiendo en forma oportuna satisfacer necesidades de información, como apoyo en el desarrollo de las actividades propias del centro. (Ruiz, 2001)

1.2.22 Dominio

Conjunto de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado un servidor de dominios.

1.2.23 DOS (MS/DOS)

Estas siglas significan Disk Operating System (DOS). Se refieren al sistema operativo (S.O.) anterior a Windows que, en su momento, creó la empresa Microsoft.

1.2.24 Equipo de cómputo

Dispositivo con la capacidad de aceptar y procesar información en base a programas establecidos o instrucciones previas, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos,

entregando resultados mediante despliegues visuales, impresos o audibles. (Villani, 2018)

1.2.25 Equipo de telecomunicaciones

Todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.

1.2.26 Filtro de paquetes

Programa que intercepta paquetes de datos, los lee y rechaza los que no estén en un formato predefinido.

1.2.27 Finger

Programa que muestra información acerca de un usuario específico, o acerca de todos los usuarios, conectados a un sistema remoto. Habitualmente se muestra el nombre y apellido, hora de la última conexión, tiempo de conexión sin actividad y terminal. Puede también mostrar archivos de planificación y de proyecto del usuario.

1.2.28 Firewall

Es un sistema diseñado para evitar accesos no autorizados desde o hacia una red privada. Los Firewalls pueden estar implementados en hardware o software, o una combinación de ambos. Los firewalls son frecuentemente utilizados para evitar el acceso no autorizado de usuarios de Internet a redes privadas conectadas a la misma, especialmente intranets. Todos los mensajes que dejan o entran a la red pasan a través del firewall, el cual examina cada mensaje y bloquea aquellos que no cumplan con determinado criterio de seguridad. (Infante, 2018)

1.2.29 Firma digital

Valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación. (SICE, 2018)

1.2.30 FTP

(File Transfer Protocol) protocolo parte de la arquitectura TCP/IP utilizado para la transferencia de archivos.

1.2.31 Gusano

Es programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos solamente realizan copias de ellos mismos. (Eliazar, 2004)

1.2.32 Hacker

Persona que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo. (Internetglosario, 2017)

1.2.33 Host

(Sistema central) computador que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet y FTP. (Echeverria, 2018)

1.2.34 HTML

Lenguaje de marcado de hipertexto, (Hyper-Text Markup Language) es el lenguaje con que se escriben los documentos en el World Wide Web. (Lamarca Lapuente, 2018)

1.2.35 HTTP

Protocolo de Transferencia de Hipertextos (Hyper-Text Transfer Protocol). Es el protocolo usado por el Word Wide Web para transmitir páginas HTML.

1.2.36 Hub

Un punto común de conexión de dispositivos en una red. Los hubs son usados comúnmente para conectar segmentos de una LAN. Un hub contiene múltiples

puertos. Cuando un paquete llega al puerto, es copiado a los otros puertos, de esta manera los otros segmentos de la LAN pueden ver todos los paquetes. Un hub pasivo simplemente sirve de conductor de datos entre los diferentes puertos. Los llamados hubs inteligentes incluyen servicios adicionales como permitir a un administrador monitorear el tráfico y configurar cada puerto del hub. Estos hubs se conocen generalmente como hubs administrables (manageable hubs). Un tercer tipo de hub, llamado switching hub, lee la dirección de destino en cada paquete y lo envía al puerto correcto. (Cabarcas, 2013)

1.2.37 Identificación

Un subtipo de autenticación, verifica que el emisor de un mensaje sea realmente quien dice ser.

1.2.38 Incidente

Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

1.2.39 Infección

Es la acción que realiza un virus al introducirse, empleando cualquier método, en nuestro ordenador (o en dispositivos de almacenamiento) para poder realizar sus acciones dañinas.

1.2.40 Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos. (Moncada, 2001)

1.2.41 Intranet

Una red privada dentro de una compañía u organización que utiliza el mismo software que se encuentra en Internet, pero que es solo para uso interno. (Cabarcas, 2013)

1.2.42 IP Address

(Dirección IP) dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos.

1.2.43 ISP

(Internet Service Provider – Proveedor de servicios de Internet) Empresa que presta servicios de conexión a Internet.

1.2.44 Local Area Network

(LAN) (Red de Área Local) red de datos para dar servicio a un área geográfica pequeña, un edificio por ejemplo, por lo cual mejorar los protocolos de señal de la red para llegar a velocidades de transmisión de hasta 100 Mbps (100 millones de bits por segundo).

1.2.45 Macro / Virus de Macro

Una macro es una secuencia de operaciones o instrucciones que definimos para que un programa (por ejemplo, Word, Excel, o Access) realice de forma automática y secuencial. Estas son "microprogramas" que pueden ser infectados por los virus. Los documentos de texto, las bases de datos o las hojas de cálculo no son programas y por ello no deberían ser infectados por ningún virus. No obstante, en cada uno de los ficheros creados con este tipo de aplicaciones se pueden definir macros y éstas sí son susceptibles de ser infectadas. Los virus de macro son aquellos que infectan exclusivamente documentos, hojas de cálculo o bases de datos que tienen macros definidas. (Segovia, 2001)

1.2.46 MAN

Metropolitan Area Network. Red de Área Metropolitana.

1.2.47 Mensaje de datos

La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama o el telefax.

1.2.48 NAT

(Network Address Translation) las direcciones NAT son utilizadas comúnmente cuando se requiere conectividad de una LAN a Internet pero solo se tiene acceso a una sola dirección IP de Internet.

1.2.49 Navegador

(Browser): término aplicado normalmente a programas usados para conectarse al servicio WWW.

1.2.50 POP

(Protocolo de Oficina de Correos - Post Office Protocol) programa cliente que se comunica con el servidor, identifica la presencia de nuevos mensajes, solicita información de los mismos y utiliza al servidor como oficina despachadora de correo electrónico cuando el usuario envía una carta.

1.2.51 Privacidad

Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos será difundidas o transmitida a otros.

1.2.52 Programas (archivos .exe y .com)

Los ficheros, documentos o archivos se componen de un nombre (cuyo número de caracteres antiguamente se limitaba a 8) y una extensión que puede no existir o contener, hasta tres caracteres como máximo. Esta extensión especifica el tipo de fichero. Si es EXE o COM, el fichero será un programa ejecutable. De esta forma si hacemos doble clic sobre él o escribimos su nombre, se realizarán determinadas acciones. (Gotzy, 2017)

1.2.53 Protocolo

Descripción formal de formatos de mensaje y de reglas que dos computadores deben seguir para intercambiar dichos mensajes.

Proxy: una substitución de direcciones, usado para limitar la información de direcciones disponibles externamente. (Sarmiento & Callejas, 2000)

1.2.54 Redireccionar

Esta acción permite aplicar un nuevo destino. En el caso de los virus, se puede hablar de éste término cuando un virus es capaz (por ejemplo) de hacer que el sistema en lugar de acceder a una dirección en la que debería encontrar determinados componentes, es obligado por el virus a saltar o acceder a otra dirección diferente. (Marly, 2007)

1.2.55 Router

(Direccionador) dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar se realiza en base a información de nivel de red y tablas de direccionamiento.

1.2.56 SATAN

(Security Analysis Tool for Auditing Networks). Herramienta de Análisis de Seguridad para la Auditoria de Redes. Conjunto de programas para la detección de problemas relacionados con la seguridad.

1.2.57 Script

Archivos con su extensión SCR que sirven para determinar los parámetros ("condiciones") con los que se deben ejecutar unos determinados programas. Permiten iniciar un programa con unas pautas fijadas de antemano.

1.2.58 Seguridad

Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados. En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación,

aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos. El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos. (Rendón, 2018)

1.2.59 Sendmail

Aplicación de administración de correo electrónico propia del sistema operativo Linux.

1.2.60 SHTTP

(Secure HTTP - HTTP seguro). Protocolo HTTP mejorado con funciones de seguridad con clave simétrica.

1.2.61 Sistema Operativo (S.O.)

Existen dos términos muy utilizados en informática. Estos son los conceptos de hardware y software. El primero de ellos se refiere a todo lo que es físico y tangible en el ordenador, como unidades de disco, tarjetas gráficas, microprocesador, memoria, etc. Por otro lado está el software que se define como el conjunto de programas (o información) con la que puede trabajar el hardware (ficheros, directorios, programas ejecutables, bases de datos, controladores, etc.). El sistema operativo pertenece al software y más concretamente es el conjunto de programas (y ficheros o archivos de otro tipo) que permite que se pueda utilizar el hardware. Se puede tener el mejor ordenador del mundo (el mejor hardware), pero si éste no tiene instalado un sistema operativo, no funcionará (ni siquiera se podrá encender). Algunos ejemplos de sistemas operativos son: MS/DOS, UNIX, OS/2, Windows 95/98/2000/NT, etc. (Pra, 2016)

1.2.62 SMTP

(Simple Mail Transfer Protocol - Protocolo de Transferencia Simple de correo). Es el protocolo usado para transportar el correo a través de Internet.

1.2.63 Spam

Envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico.

1.2.64 SSL

(Secure Sockets Layer - Capa de Socket Segura). Protocolo que ofrece funciones de seguridad a nivel de la capa de transporte para TCP.

1.2.65 TCP

(Transmission Control Protocol - Protocolo de control de Transmisión). Uno de los protocolos más usados en Internet. Es un protocolo de capa de transporte.

1.2.66 Telnet

Telnet es el protocolo estándar de Internet para realizar un servicio de conexión desde un terminal remoto.

1.2.67 Texto Plano

(Plain Text) se llama así al documento antes de ser encriptado.

1.2.68 Trojan Horse

(Caballo de Troya) programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema que lo procesa.

1.2.69 URL

(Localizador Uniforme de recursos - Uniform Resource Locator). Sistema de direccionamiento estándar para archivos y funciones de Internet, especialmente en el Word Wide Web. El URL está conformado por el servicio (p. e. http://) más el nombre de la computadora (p. e. www.sfp.gob.pe) más el directorio y el archivo referido. (Galeon, 2018)

1.2.70 WAN

Wide Area Network. Red de Area Extensa.

1.2.71 Webmin

Es una aplicación con interface gráfica para la administración de sistemas Unix.

1.2.72 WWW

World Wide Web. Estrictamente la Web es la parte de Internet a la que accedemos a través del protocolo HTTP y en consecuencia gracias a browsers normalmente gráficos como Netscape o Internet Explorer. (Sottile, 2016)

1.3 Antecedentes

Cerini y Prá (2002) el objetivo general de una evaluación a la seguridad consiste en la realización de una Auditoría Informática en la empresa, esto con el fin de relevar las vulnerabilidades existentes en lo relativo a controles de seguridad, como medio para el desarrollo de una Política de Seguridad, donde se definirán los lineamientos para promover la implementación de un modelo de seguridad en toda la organización.

La investigación concluye en lo siguiente: A lo largo del presente trabajo pudimos comprender que la seguridad en cómputos es un conjunto de recursos destinados a lograr que la información y los activos de una organización sean confidenciales, íntegros y disponibles para todos sus usuarios.

Pallas (2009) menciona que el ámbito de aplicación de la seguridad es amplio en el sentido que alcanza a grupos empresariales y organizaciones donde existe una relación jerárquica o de subordinación, relación que condiciona la gestión de la seguridad de la información y que debe incorporarse como tal a un SGSI. Este trabajo, y la metodología que en él se propone, se centra en una empresa subordinada como parte constitutiva de un grupo empresarial jerárquico, donde existe otra, que denominaremos principal. Ésta última, eventualmente podría tener ya, un SGSI implantado y será considerada en cuanto al contexto y cómo condiciona al SGSI de la primera, pero no será el objeto principal de análisis. La metodología tiene un amplio campo de aplicación, donde exista una relación de dependencia o integración vertical entre empresas. También puede aportar aspectos metodológicos, en lo referente a la jerarquización de los lineamientos de seguridad, para una entidad gubernamental en su rol de regular o generar lineamientos y/o (meta) políticos en seguridad de la información para empresas y organismos estatales. No obstante, concluye que no es el fin perseguido en su trabajo sino aportar una metodología con esta

concepción de enfoque global y sistémico, atendiendo a la pertenencia de la empresa a un grupo empresarial, y a su vez pragmático, a los efectos que la misma sea, no sólo viable, sino conveniente y efectiva, dando una estructura u organigrama para lograr la coordinación necesaria y especificando los procedimientos que deben cumplirse en cada fase, promoviendo no sólo la reutilización y coherencia integral de la seguridad sino también fomentando la sinergia entre las empresas del grupo. Un producto parcial y homónimo de este trabajo de tesis, se ha constituido en una ponencia en el marco del "V Congreso Iberoamericano de Seguridad Informática (CIBSI'09)" en Montevideo, Uruguay, en noviembre de 2009.

Ferrero (2009) menciona que como base para una seguridad efectiva de TI, se deben formular objetivos, estrategias y políticas generales de seguridad de la organización. Estos proporcionan soporte a la actividad de la organización y aseguran la consistencia entre todas las salvaguardas. Los objetivos identifican lo que se debe lograr, las estrategias, cómo conseguir estos objetivos, y las políticas, lo que debe hacerse. Los objetivos, estrategias y políticas se pueden desarrollar jerárquicamente desde el nivel más alto hasta el nivel operativo de la organización. Así mismo dichos niveles han de guardar una relación consistente que permita relacionarlos de forma clara. Lo primero a realizar es la definición concreta del sistema y el alcance que este posee, la importancia que tiene para la organización. Un vez establecido dicho alcance se han de estudiar y plantear los objetivos y estrategias que se van a adoptar para la seguridad del sistema de TI. Valiéndose de los objetivos y estrategias acordadas se obtienen una serie de políticas de seguridad de TI para la organización. La política de seguridad de la organización consta de los principios y directrices de seguridad de la organización como un todo. La política de seguridad de TI debe reflejar los principios y directrices de seguridad esenciales aplicables a la política de seguridad de la organización y al uso general de los sistemas de TI dentro de la misma. La política de seguridad de un sistema de TI concreto debe reflejar los principios y directrices expresados en la política de seguridad de TI de la organización. Debería contener los requisitos particulares de la seguridad y de las salvaguardas que deben implantarse y de cómo usarlas correctamente para garantizar la seguridad adecuada. En todos los casos es importante que el enfoque adoptado sea coherente con las necesidades debidas a la actividad de la organización.

Donde se concluye que: A lo largo de este proyecto se ha intentado dar a conocer la importancia del funcionamiento y la seguridad (en sus aspectos de confidencialidad,

integridad y disponibilidad) de los sistemas de información en las empresas y las organizaciones debido a que, cada vez más, las TI (Tecnologías de la Información) y la información son más imprescindibles en sus procesos de negocio. Para ello se ha explicado la importancia de realizar un Análisis y Gestión de Riesgos en aquellos sistemas cuya importancia para el correcto funcionamiento de la organización es vital. Realizar un AGR es una tarea costoso en tiempo y esfuerzos, por ello hay que saber hasta dónde se quiere abarcar, que se va a tener en cuenta y que tipo de AGR se va a realizar. En este proyecto se ha aplicado una metodología específica para llevar a cabo esta tarea: Magerit. Aplicar un método como el propuesto por Magerit es costoso en tiempo pero efectivo a la hora de llevar a cabo todos los pasos sin dejar nada a la improvisación o al descuido. Otra gran ventaja de aplicar Magerit es la posibilidad que se ha tenido de usar una herramienta informática diseñada específicamente para Magerit. Esta herramienta, EAR, ha facilitado el análisis, el retroceso en los casos en los que sido necesario, ha permitido automatizar muchas de las tareas que sin EAR hubiesen supuesto un gran esfuerzo (generación de informes, mapas, esquemas, etc.).

Matalobos (2009) propone enmarcar en el desarrollo, por parte de la Organización, de un Plan Director de Seguridad de Información y un sistema de Seguridad de Información, cuyo desarrollo se ha definido como parte del Plan Estratégico Corporativo.

Específicamente, su proyecto ha consistido en la realización de un análisis de riesgos de seguridad de la información que permita cuantificar y comparar los requerimientos de seguridad de la información de la Organización con los controles implantados para su cumplimiento, y, en base a las diferencias encontradas, definir los controles adicionales necesarios para cumplir con los requerimientos.

Para el desarrollo de este proyecto se ha definido una metodología de trabajo desarrollada a medida y basada en las principales metodologías de análisis y gestión de riesgo de uso habitual en el mercado de la seguridad de la información y en las necesidades, cultura y estructura específicas de la Organización.

Una vez definida la metodología se ha diseñado y desarrollado una herramienta informática de soporte, que permita aplicar la metodología de forma eficaz y eficiente.

Finalmente, tanto la metodología como la herramienta se han empleado en la realización del análisis de riesgos planteado como objetivo del proyecto.

Donde se concluye que: Se han identificado los principales activos de la información de la Organización en términos de los requerimientos de la seguridad definidos, lo que ha permitido identificar las áreas que requieren mayor atención, diferenciándolas de aquellas para las que puede ser suficiente el baseline actual de la seguridad.

Román (2002) presenta nociones de seguridad y otros conceptos necesarios para una buena comprensión del análisis de seguridad que se llevan a cabo en portales web.

El sector de la seguridad informática es muy amplio, y abarca muchos y diversos campos. “Podríamos escribir libros y libros sobre el tema, pero como es natural no lo haremos; necesitamos centrar nuestros objetivos. Colocaremos nuestro punto de mira sobre el tema de la seguridad en servidores web, e intentaremos no desviarlo demasiado, salvo en situaciones especiales que requieran dar una visión más global de ciertos conceptos que contribuyan a un mejor entendimiento de otros puntos explicados con anterioridad. Una vez leído este capítulo, el lector será conocedor de algunas de las técnicas más comunes de explotación de agujeros de seguridad vía web, y quién sabe, lo mismo le pica el gusanillo y se acaba convirtiendo en aprendiz de hacker”, indican los autores.

CAPÍTULO II

PLANTEAMIENTO DEL PROBLEMA

2.1 Planteamiento de la investigación

En el IESTP – Acora cuenta con un Sistema Académico desarrollado con un lenguaje de programación de web, el lenguaje de programación utilizado es “PHP” (Por observación del investigador), el motor de base de datos que sirve como soporte para la aplicación fue desarrollado en MySQL (Por observación del investigador). La integridad de la información es vital en cualquier organización, es así que las consecuencias de fallo en el sistema pueden causar pérdidas de información vitales para los alumnos que están cursando sus estudios en la institución, la complejidad del software es de vital importancia en este tipo de sistemas, debido a que semestralmente se registra una gran cantidad de información al sistema, otro factor es la exposición alta de los datos a usuarios comunes que no tienen relación con la oficina de secretaría académica.

Según las entrevistas personales realizadas al encargado de la oficina de secretaría académica, a la pregunta ¿Se han identificado y evaluado los riesgos del sistema?, su respuesta fue la siguiente: “No se ha identificado ni realizado ningún tipo de peligros que puede ocasionar el uso del sistema, aún no sabemos si este puede impactar negativamente sobre la institución o que algún mal uso del sistema pueda provocar que este falle repentinamente” (Entrevista personal realizada al responsable de la oficina de secretaría académica)

Es necesario el uso de sistemas en la vida cotidiana del encargado de la oficina de secretaría académica, pero sin embargo también es necesario brindar la seguridad que la información está siendo resguardada celosamente y no será fácilmente violada por un tercer ente.

Siendo la seguridad del software “Una actividad de garantía de calidad de software que se centra en la identificación y evaluación de riesgos potenciales que puede producir un impacto negativo en el software” (Pressman, 1982).

El Sistema Académico es de suma importancia en estos tiempos para las instituciones, sean instituciones públicas o privadas. Los niveles de la educación tanto primaria, secundaria y superior están bajo la tutela del Ministerio de Educación, de los cuales solo han sido tomados en cuenta para tener un sistema académico los niveles de inicial primaria y secundaria, el sistema se denomina SIAGIE (Sistema de Información de Apoyo a la Gestión de la Institución Educativa) sistema monitoreado por el Ministerio de Educación a nivel nacional, sin embargo una realidad preocupante es que los Institutos de Educación Superior tanto Tecnológicos, Pedagógicos ESFAS y CETPROS, siendo parte del Ministerio de Educación no hayan sido considerados para tener un sistema académico y siendo abandonados tanto a nivel regional así como a nivel nacional, y aún lo más contradictorio es que el IESTP – Acora teniendo una especialidad de computación e informática no hayan desarrollado ni en lo mínimo un sistema académico de primer nivel con estándares de seguridad.

¿Cuál es el nivel de seguridad del sistema académico del Instituto Superior Tecnológico Acora?

2.2 Objetivos

2.2.1 Objetivo general

Evaluar el sistema académico del Instituto de Educación Superior Tecnológico Público Acora.

2.2.2 Objetivos específicos

- Realizar la evaluación de la seguridad lógica.
- Realizar la evaluación de la seguridad en comunicaciones.
- Realizar la evaluación de la seguridad de las aplicaciones.
- Realizar la evaluación de la seguridad física.
- Realizar la evaluación de las auditorias y revisiones.

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1 Tipo del problema de investigación

Debido a las características de la muestra y al problema de la investigación, se trata de un tipo de Investigación descriptivo, que tiene como propósito medir el nivel de seguridad del sistema académico considerando el problema en estudio y sus componentes, este concepto se ajusta a la definición brindada por Hernández *et al.* (2014), acerca de los estudios descriptivos.

3.2 Población de la investigación

La población está dada por estudiantes, docentes y la plana administrativa del Instituto de Educación Superior Tecnológico Público Acora, con el siguiente detalle:

- 01 Director General.
- 01 Jefe de Área Académica.
- 03 Jefes de Área.
- 13 Docentes.
- 03 Personal Administrativo.
- 178 Estudiantes.

3.3 Muestra de la investigación

La muestra es el subconjunto representativo de la población.

Por lo tanto, la muestra seleccionada corresponde al siguiente detalle:

- 01 Director General.
- 01 Jefe de Área Académica.
- 01 Jefe de Área.
- 05 Docentes.
- 01 Personal Administrativo.
- 50 Estudiantes.

La muestra corresponde a tipo "No Probabilística" la cual fue determinada, por conveniencia, debido a los objetivos y criterios del investigador. Las cuales se señala por los siguientes criterios:

- El número de docentes de la Institución Educativa es muy reducido.
- Por el número menor a 500 sujetos de la población, no se aplica la fórmula muestral.

"En las muestras no probabilísticas, la elección de los elementos no depende de la probabilidad, sino de causas relacionadas con las características de investigación del investigador o el que hace la muestra, por lo que depende del proceso de toma de decisiones de una persona o de Grupo de persona". (Hernández *et al.*, 2014).

3.4 Ubicación y descripción de la población o ámbito de estudio

- Departamento: Puno.
- Provincia: Puno.
- Distrito: Acora.
- Instituto de Educación Superior Tecnológico Público Acora de la DRE Puno.

3.5 Técnicas e instrumentos para recolectar información

Con esta técnica de recolección de datos pudimos establecer contacto con los Docentes, Jefes y Director de la Institución Educativa Superior, por medio de cuestionarios previamente establecidos. Luego se precedió al análisis e interpretación de los resultados

obtenidos con el fin de cumplir con la evaluación de la seguridad lógica, seguridad de comunicaciones, seguridad de las aplicaciones, seguridad física y con la evaluación de las auditorías y revisiones, según

Para la recolección de datos se utilizó distintas evaluaciones (según las variables estudiadas), como son, la evaluación de la seguridad lógica, seguridad de comunicaciones, seguridad de las aplicaciones, seguridad física, evaluación de las auditorias y revisiones. Luego, se procedió al análisis de la información obtenida con la finalidad de cumplir con los parámetros que exige la normatividad y los estándares y guías de COBIT (Control Objetive for Informatión Technology), ISO 17799 (British Standard 7799).

3.5.1 Encuestas

La encuesta sirvió para recolectar datos y dar lugar a establecer contacto con las unidades de observación por medio de cuestionarios previamente establecidos. La modalidad empleada fue la de encuesta personal el cual nos permitió conocer el entorno y el fenómeno sin modificarlo, el recojo de la información sirvió para el análisis de la situación real. Los datos fueron obtenidos por un conjunto de preguntas normalizadas y dirigidas a la muestra respectiva, obteniendo opiniones, ideas, características y hechos específicos.

3.5.2 Entrevistas.

La entrevista nos permitió obtener una situación de interrelación y dialogo entre el entrevistador y el entrevistado. Entre las modalidades que subjetivamente empleamos para la entrevista tenemos que resaltar que la más empleada fue la entrevista estructurada y semiestructurada.

3.5.3 Análisis documental

El análisis documental es un conjunto de operaciones encaminadas a representar un documento y su contenido bajo una forma diferente de su forma original, con la finalidad posibilitar su recuperación posterior e identificarlo.

El análisis documental para la recolección de información fue de importancia para recolectar documentos necesarios para su procesamiento intelectual que dio lugar a la obtención de documentos principales y/o secundarios que actúa como

intermediario o instrumento de búsqueda obligado entre el documento original y el usuario que solicita información. El calificativo de intelectual se debe a que el documentalista debe realizar un proceso de interpretación y análisis de la información de los documentos y luego sintetizarlo.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1 Informe de relevamiento

La Institución estudiada auditada, Instituto de Educación Superior Tecnológico Público Acora, es una institución, con 178 estudiantes, divididos en tres carreras profesionales, Computación e informática, enfermería técnica y producción agropecuaria.

A continuación, se describen los datos y la información recogida durante el relevamiento realizado al IESTP – Acora, detallando cada uno de los controles que se implementan en la actualidad.

4.1.1 Seguridad lógica.

Objetivo de auditoría: los auditores deberán evaluar los controles de accesos de los usuarios al sistema informático académico y a los datos que éstas gestionan, con el fin de señalar las irregularidades que obstaculicen la confidencialidad, exactitud y disponibilidad de la información, y las mejoras que fueran factibles de efectuarse.

4.1.1.1 Identificación de usuarios

Altas docentes

Cuando un usuario nuevo ingresa a la Institución, el área de Administración toma sus datos, dando de alta su resolución, sin embargo, no existe un procedimiento formal a seguir para realizar estas tareas. Este usuario necesita del sistema informático académico, entonces secretaría académica hace el pedido de la información del nuevo usuario a la oficina

de administración, luego la secretaria de genera un acceso para luego acceder al módulo de registro en donde se genera el alta del usuario al sistema.

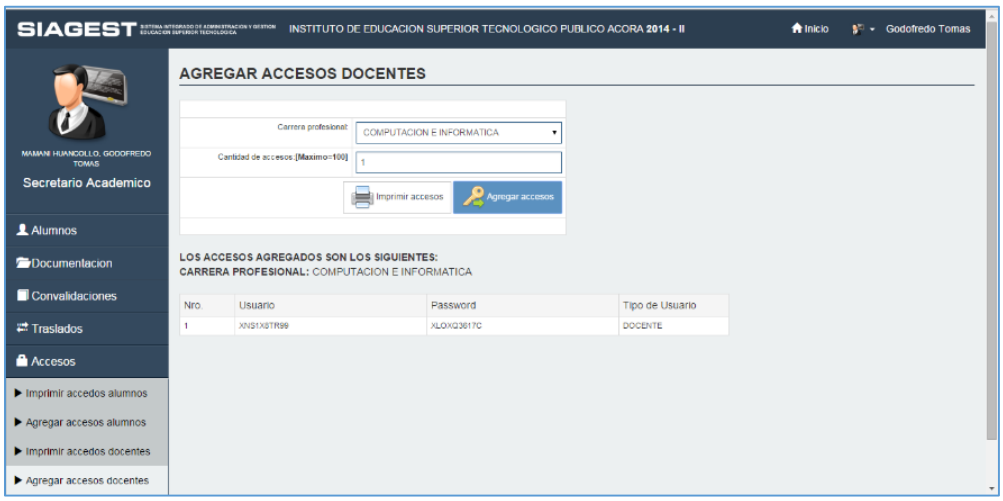

Figura 1. Generación de accesos docente módulo de secretaria académica

Luego de generar el acceso el secretario académico accede al módulo de registro de docentes, ingresando los datos de acceso generados.

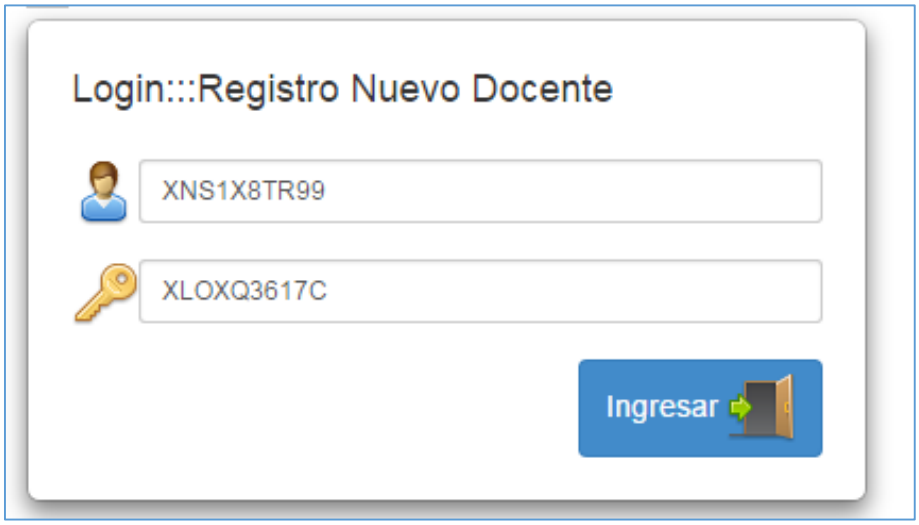

Figura 2. Login para alta de docentes

Los datos que se ingresan en la cuenta son los siguientes:

- **ID del Usuario:** es un número autogenerado luego de realizar la alta.
- **Carrera:** es una de las carreras que pertenecen a la institución.

- **Codigo Modular:** el código modular en la mayoría de los casos es el número de DNI antecedido por un número 10, en otros casos el código modular viene a ser el código de plaza.
- **Condición Laboral:** la condición laboral puede ser Nombrado, Contratado o Destacado.
- **Dicta en Otras Carreras:** este campo pide indicar si el docente a dar de alta va a dictar clases en otras carreras o solamente dicta clases en la carrera indicada.

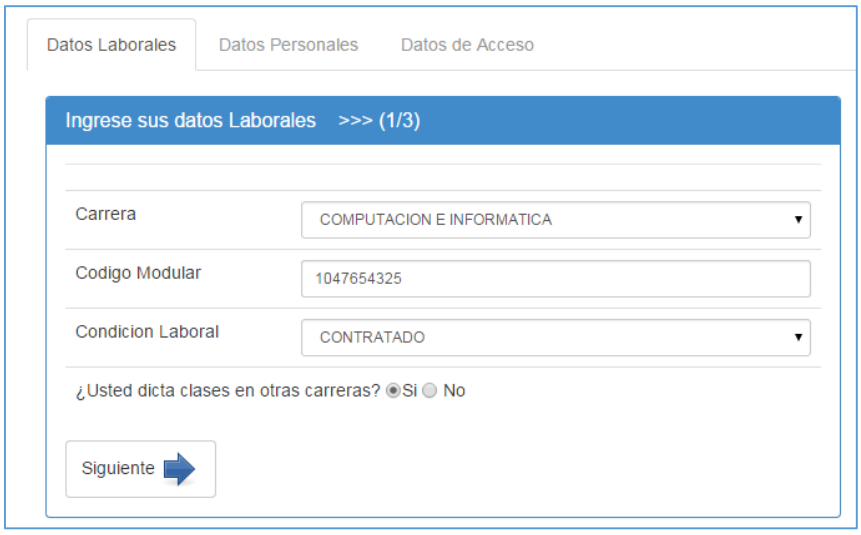

Figura 3. Ingreso de datos laborales del docente

- DNI: se ingresa el documento nacional de identidad.
- Nombres y Apellidos: se obtienen de la oficina de Administración.
- Sexo: Masculino o Femenino.
- Correo Electronico: se ingresa el correo electrónico del docente.
- Dirección: Se consigna la dirección actual del docente, indicando el distrito, provincia y departamento.
- Telefono: Se condigna el teléfono o celular actual del docente.
- Foto: Es una opcional si el docente desea subir o no su foto al sistema.

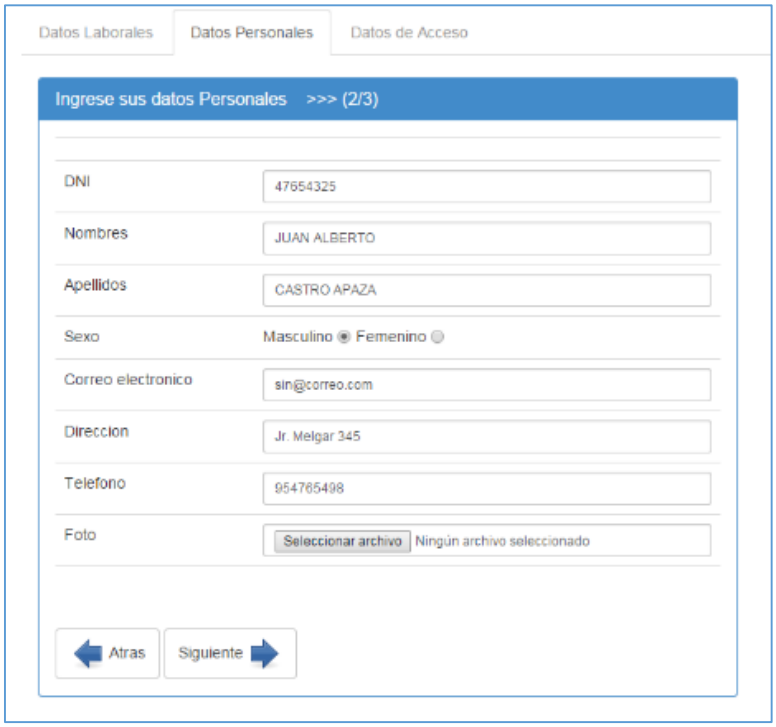

Figura 4. Ingreso de datos personales del docente

- Usuario: Se sistema verifica que el usuario no exista en la base de datos del sistema, en caso que el sistema encuentre el usuario se muestra un mensaje con las indicaciones respectivas.
- Clave: Se ingresa el mismo usuario repitiéndolo dos veces, indicando al usuario que la contraseña sebe de ser cambiada lo más pronto posible.

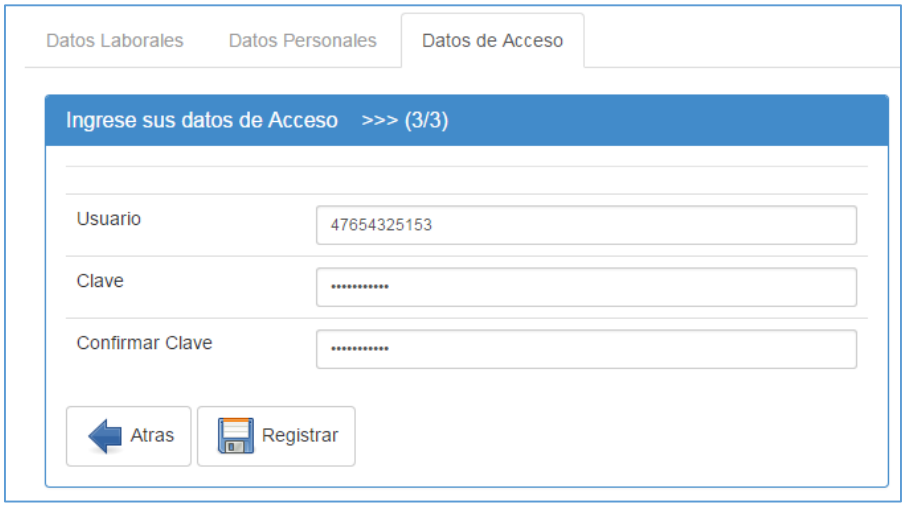

Figura 5. Ingreso de datos de acceso

Internamente se registran los siguientes datos.

- Grupo al que Pertenece: Según sus funciones se le registra en el grupo de Alumnos, Docentes, Secretario Academico o Jefe de Area.

Existe un módulo para asignar los cargos administrativos en el sistema, el responsable de realizar los cambios es el secretario académico.

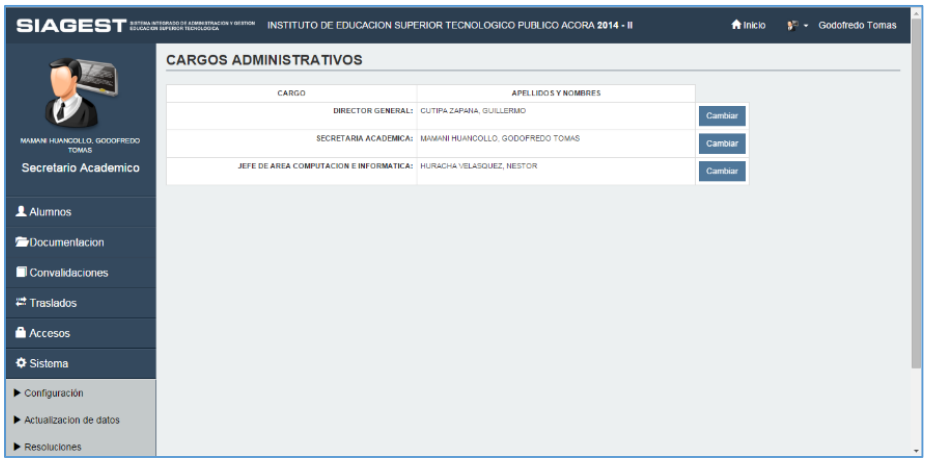

Figura 6. Asignación de cargos administrativos

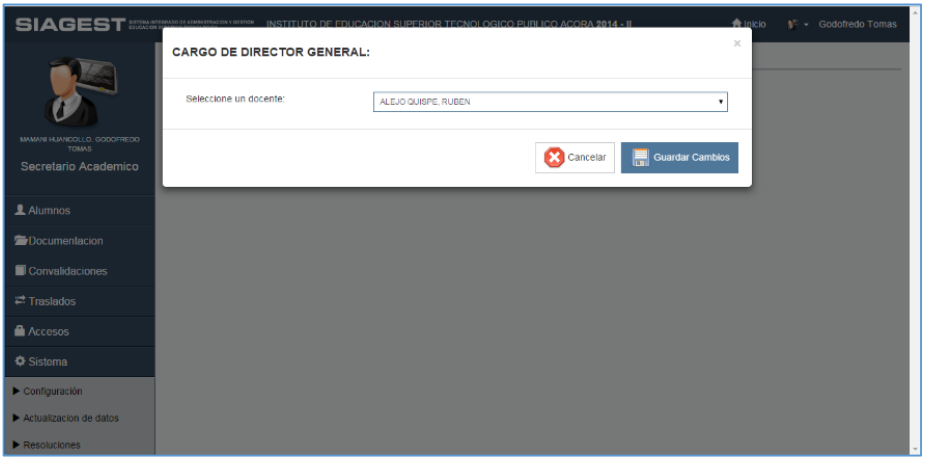

Figura 7. Modo de cambiar cargo administrativo

- Fecha de Desactivación de la Cuenta: La cuenta es desactivada una vez que el usuario ya no tiene ningún tipo de vínculo con la institución.

Existe un módulo para realizar la operación de vínculo laboral activo o inactivo, dicho módulo está a cargo del secretario académico.

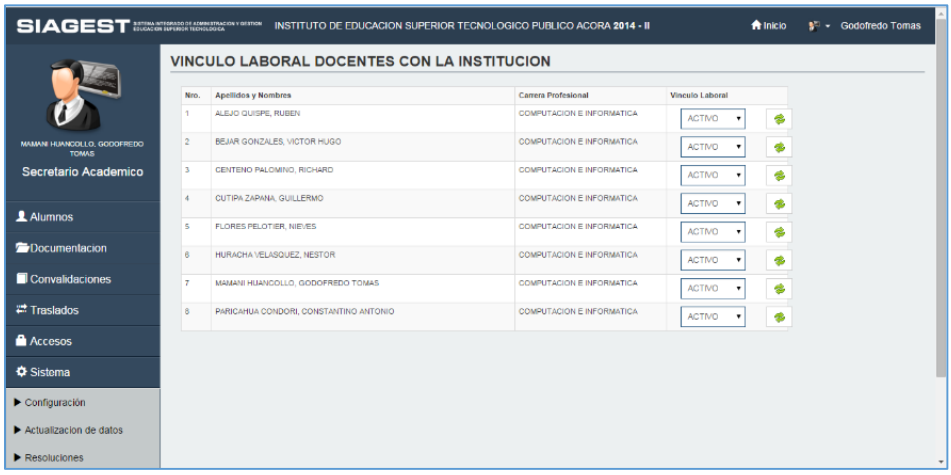

Figura 8. Vínculo laboral con la institución

- Contador De Intentos Fallidos No existe ningún contador de intentos fallidos por parte del sistema.

- Restricciones Horarias para el uso del Sistema: No existen restricciones algunas para usar el sistema, ya que este está alojado en un servidor web en internet el acceso es en cualquier momento.

- Documentos Imprimibles: Existen restricciones para poder imprimir documentos, esto depende del tipo de usuario y la información que este maneje, solamente pueden imprimir documentos que les concierne y se encuentra entre sus funciones.

Los documentos que se pueden imprimir están en formato PDF, lo cual hace difícil la tarea de poder modificar la información reportada, aquí les mostramos un reporte que genera el sistema.

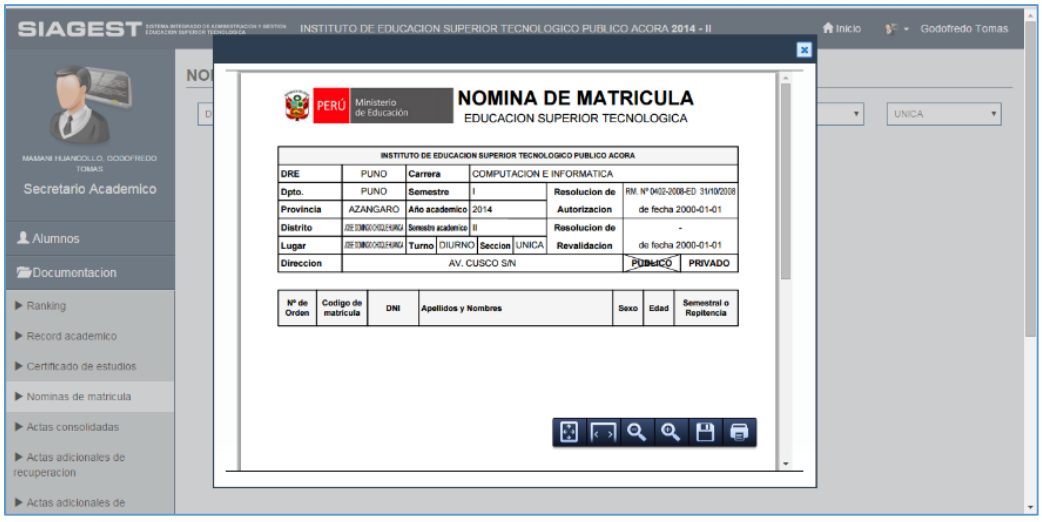

Figura 9. Ejemplo de reporte en formato PDF.

Altas estudiantes

Un usuario estudiante ingresa a la institución luego que aprueba el examen de admisión que celebra la institución, a comienzos de años, cuando un usuario nuevo ingresa a la Institución, el área de secretaria académica se encuentran registrados sus datos de inscripción. Este usuario necesita del sistema informático académico, entonces secretaría académica registra a los alumnos mediante el uso de una herramienta que le proporciona el sistema y mediante su cuenta de acceso al sistema, para dar de alta a los alumnos el secretario académico llena un formato XLS (Excel) para subirlo al sistema, luego de llenar el formato Excel el el secretario académico carga el modulo y sube a los alumnos, de esa manera se genera el alta de los usuarios alumnos al sistema.

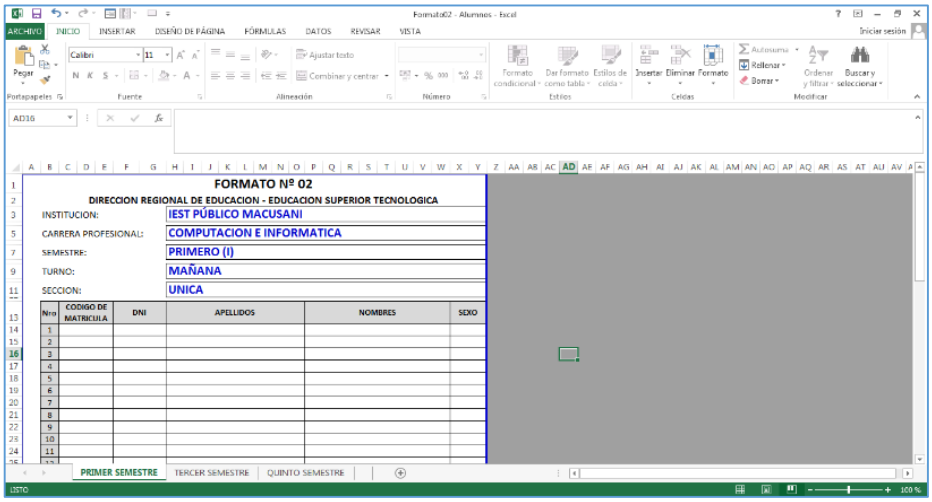

Figura 10. Formato Excel

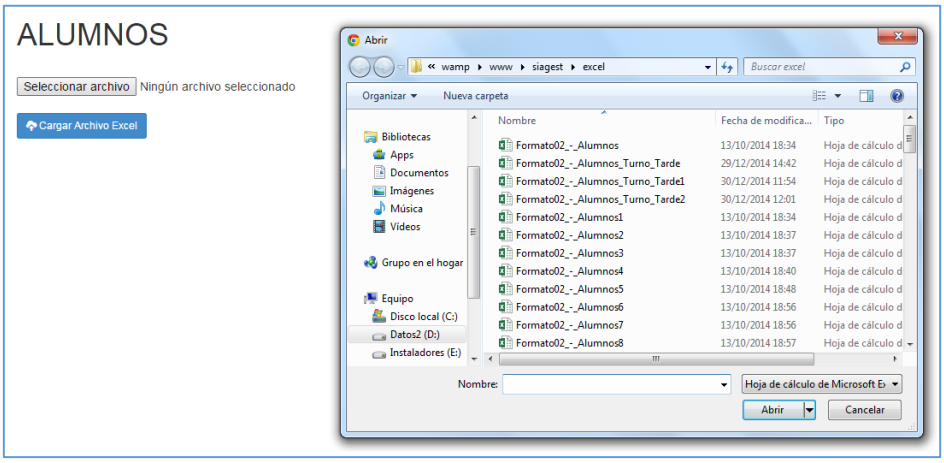

Figura 11. Módulo para dar de alta a los usuarios alumnos en masa

Altas estudiantes

Cuando es necesario dar de alta solamente a un estudiante se puede emplear el módulo de registro alumnos, en donde el alumno entrega sus datos de forma personal en una entrevista con el secretario académico, para tal efecto la secretaría académica primeramente debe de generar un acceso para luego acceder al módulo de registro en donde se genera el alta del usuario estudiante en el sistema.

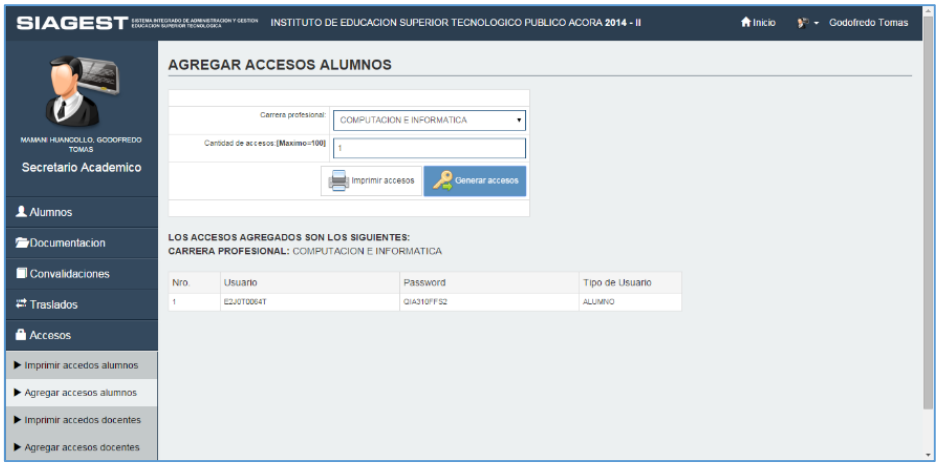

Figura 12. Generación de accesos alumnos, módulo de secretaria académica

Una vez que el acceso ha sido generado, el secretario académico ingresa al módulo de registro alumnos e ingresa los datos generados.

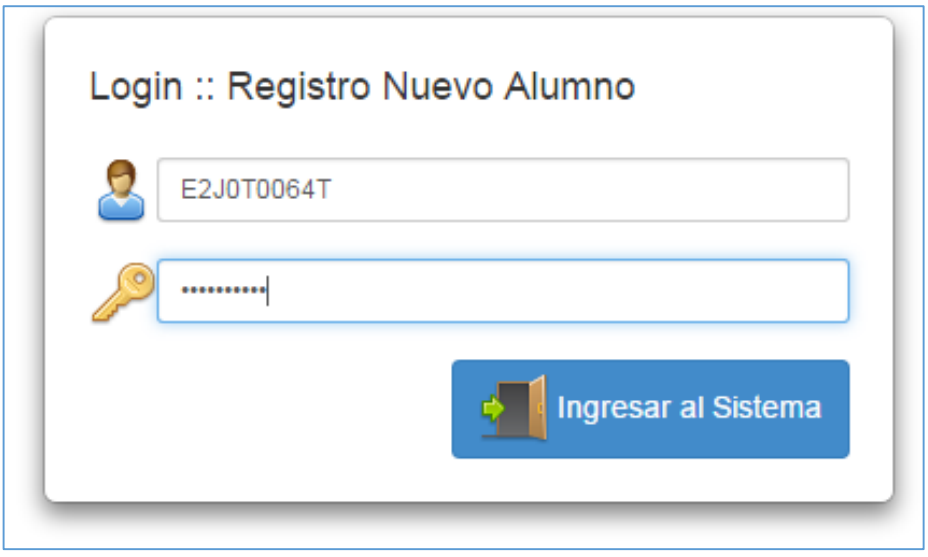

Figura 13. Login para el acceso generado, registró de nuevo alumno

Los datos que se ingresan en la cuenta son los siguientes:

- Código De Matricula: El código de matrícula es un código único para un alumno en la institución, dicho código es asignado por el secretario académico de la institución.
- Carrera Profesional: La carrera profesional es una de las carreras que existen en la institución.
- Semestre a Cursar: Se tiene que ingresar el semestre al cual va a pasar a estudiar según el semestre académico de la institución.
- Usuario: El nombre de usuario viene a estar dado por el número de su DNI precedido de un código que la institución genera.
- Clave: Se ingresa el mismo usuario repitiéndolo dos veces, indicando al usuario que la contraseña sebe de ser cambiada lo más pronto posible.

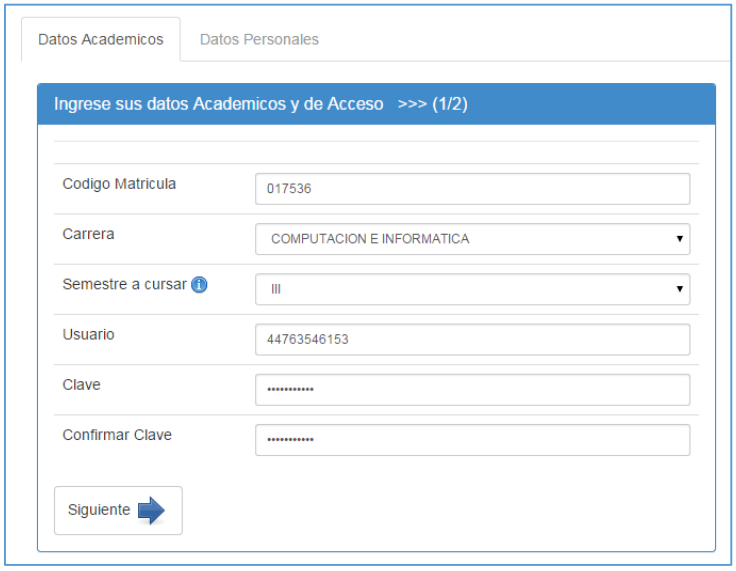

Figura 14. Registro de datos académicos del alumno

- DNI: Se ingresa el número del documento nacional de identidad.
- Nombres Y Apellidos: Se obtienen de la oficina de Administración.
- SEXO: Masculino o Femenino.
- Correo Electronico: Se ingresa el correo electrónico del docente.

- Dirección: Se consigna la dirección actual del docente, indicando el distrito, provincia y departamento.
- Celular: Se condigna el teléfono o celular actual del docente.

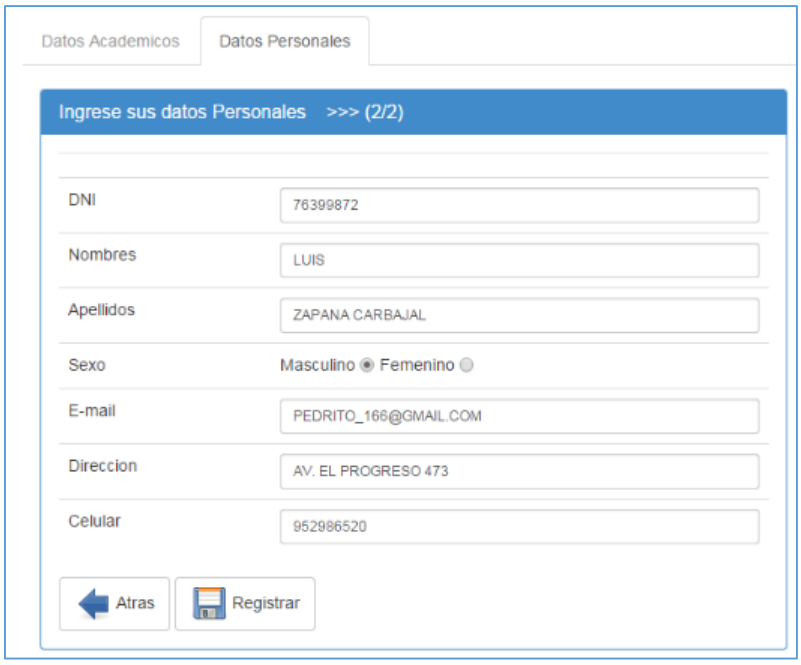

Figura 15. Registro de datos personales el alumno

Bajas

Las cuentas de usuario no se eliminan del sistema, se desactivan una vez que ya no existe ningún tipo de vínculo con la institución. De esta forma los datos de las cuentas dadas de baja quedan almacenados en la base de datos y no es posible repetir los ID generados automáticamente para nuevos usuarios.

No hay ningún procedimiento formal para dar de baja a los usuarios del sistema, la oficina de administración da a conocer si existe algún usuario que ya no tiene ningún vínculo con la institución.

Mantenimientos

No se llevó a cabo ninguna revisión periódica ni control sobre el buen funcionamiento de las cuentas de los usuarios, ni sobre los permisos que tienen signados.

Permisos

El control de acceso en la institución se basa en los perfiles de los usuarios y la asignación o denegación de permisos a los mismos, así como también en los perfiles de grupos.

Estos grupos se generan en concordancia con las áreas de la institución y en la oficina de Administración el que asigna cada usuario a un grupo determinado. Luego, los usuarios son dados de alta en el sistema, y el sistema asigna automáticamente las funciones a desempeñar en el sistema.

El sistema informático está desglosado en cuatro módulos diferentes, donde cada uno de ellos es un programa en sí mismo. De esta manera cada usuario del sistema, según el grupo al que pertenece en la organización, dispone de los accesos directos a los programas que corresponden a su área. Así, los usuarios solo pueden interactuar con los datos a los que dichos módulos les permiten acceder. Los accesos directos a los que el usuario tiene acceso los genera el sistema automáticamente, una vez que el usuario fue dado de alta.

Figura 16. Entorno de ingreso al sistema por módulos

De acuerdo a la responsabilidad del usuario en la institución es mayor, son necesarios más datos, y por ende más sub módulos, o accesos a programas. Esto quiere decir que en un cargo secretario académico puede haber 29 sub módulos disponibles, mientras que, a modo de ejemplo, los docentes solo tienen 5 sub módulos.

No existe en el sistema informático una lista de control de acceso que se utilice para identificar los tipos de permiso que tiene cada usuario con respecto a los datos. Solo existe una relación entre los sectores de la institución, los menús y los usuarios correspondientes a cada sector, y en las carpetas de documentación del desarrollo relativas a cada módulo de programa se explica la relación que existe entre cada módulo de programa y los datos. Al no existir esta lista de control de acceso, resulta complicado identificar qué datos puede modificar cada usuario.

No se tiene en cuenta ninguna restricción horaria para el uso de los recursos. Tampoco se considera una restricción física sobre la máquina desde donde se logea cada usuario.

Inactividad

Si el usuario permanece un período de tiempo logeado sin actividad, el sistema no ejecuta ninguna acción; los administradores solo advierten a los usuarios sobre la necesidad de no dejar las máquinas logeadas e inactivas. Si las cuentas de usuarios permanecen varios días sin actividad, por licencias o por vacaciones no pasan a un estado de suspensión.

El usuario root se logea en los servidores durante las 24 horas del día, debido a que éstos equipos no se apagan en ningún momento.

Cuentas de usuario

Los usuarios estudiantes no son identificados en forma personal, sino que usan todos los números de sus DNIs precedido de un código que genera el sistema, para ingresar al sistema informático.

Los módulos del sistema permiten hacer consultas a las bases de datos, (notas, horarios, datos personales, etc.) generalmente desde cualquier ambiente donde cuenten con acceso a internet.

Los usuarios del sistema pueden tener abiertos, al mismo tiempo, todos los menús a los que están autorizados, y varias sesiones del mismo menú. No se hacen restricciones en cuanto a la cantidad de sesiones que los usuarios pueden utilizar simultáneamente.

En la institución hay una persona encargada de la secretaria académica con un usuario y contraseña, encargada de la parte administrativa del sistema con tareas preestablecidas por el sistema. Además, el secretario académico puede logearse desde cualquier punto con acceso a internet, lo que resulta riesgoso ya que podría, por error, abandonar ese puesto de trabajo dejando un acceso logeado con su usuario secretario académico.

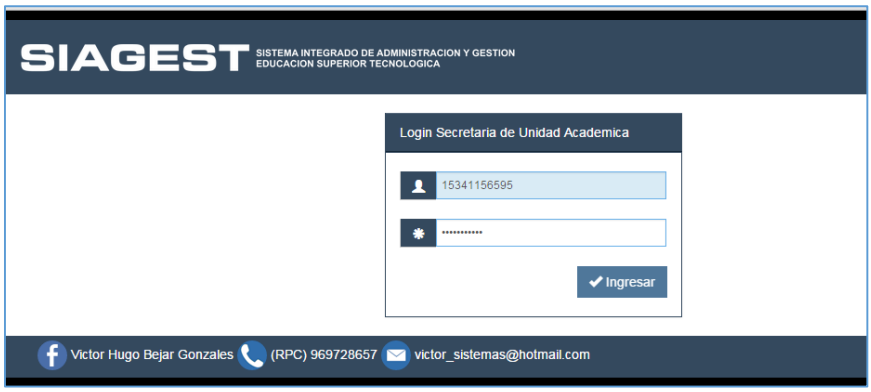

Figura 17. Login Usuario Secretario académico

Entre las funciones que el secretario académico tiene son las de:

- Realizar matriculas.

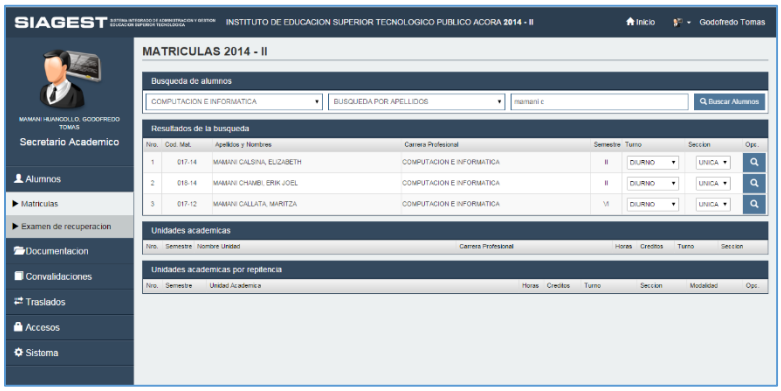

Figura 18. Matricula de alumnos

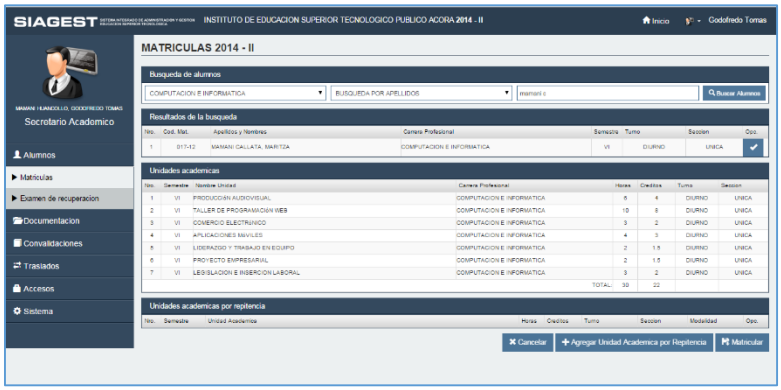

Figura 19. Elección de un alumno para su matricula

- Administrar Exámenes de recuperación.

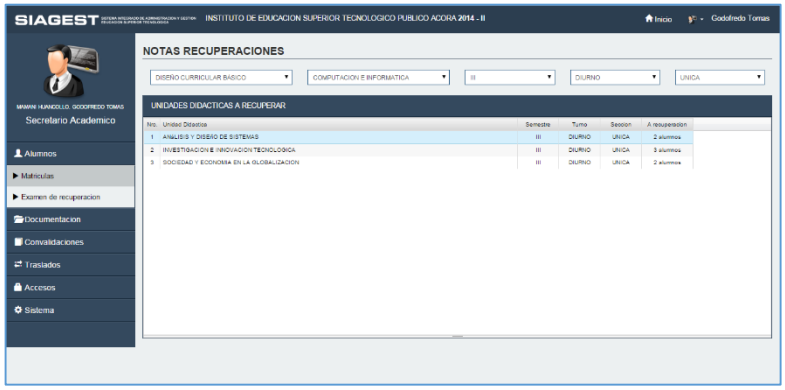

Figura 20. Administrar exámenes de recuperación

- Obtener Ranking de Notas

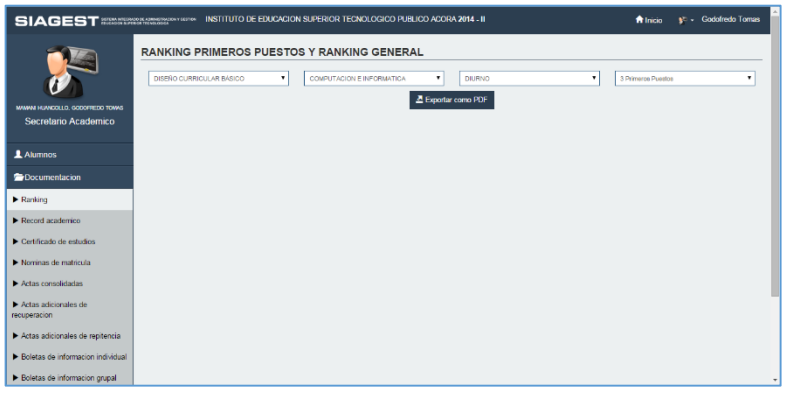

Figura 21. Formulario para reportar ranking

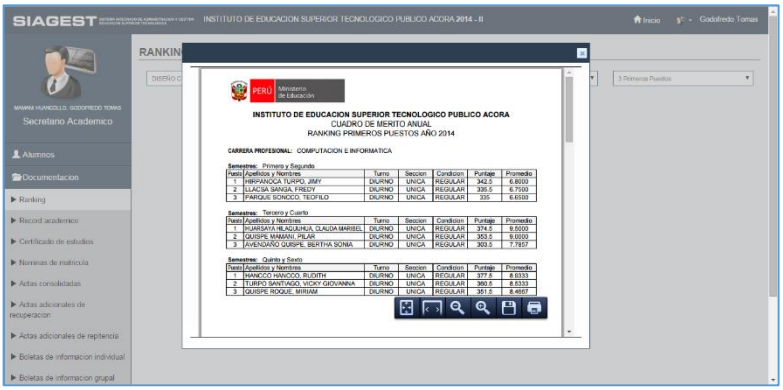

Figura 22. Reporte de Ranking

- Obtener Record Académico

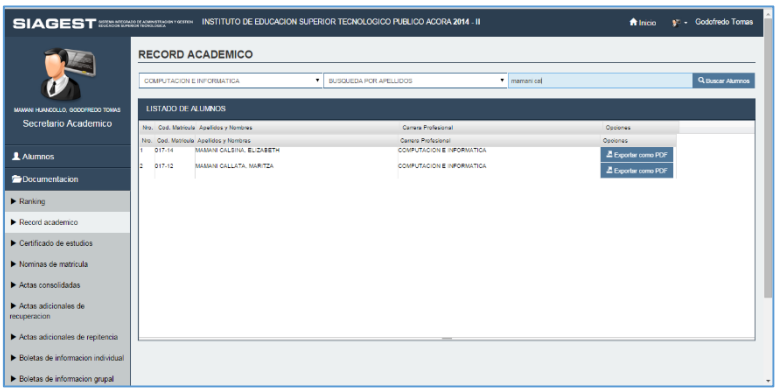

Figura 23. Formulario para obtener el record académico

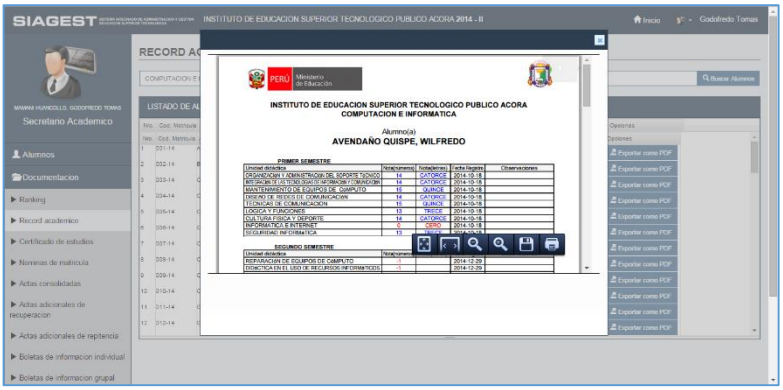

Figura 24. Reporte de record académico

- Reportar Nóminas de matrículas

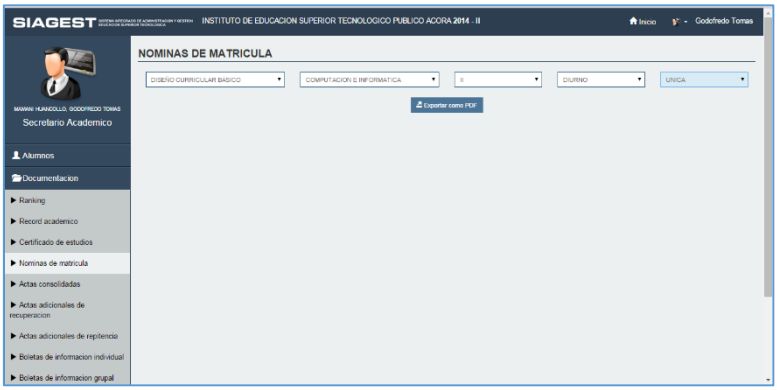

Figura 25. Formulario para reportar nóminas de matrícula

Figura 26. Reporte de nóminas de matrícula

- Reportar Actas consolidadas

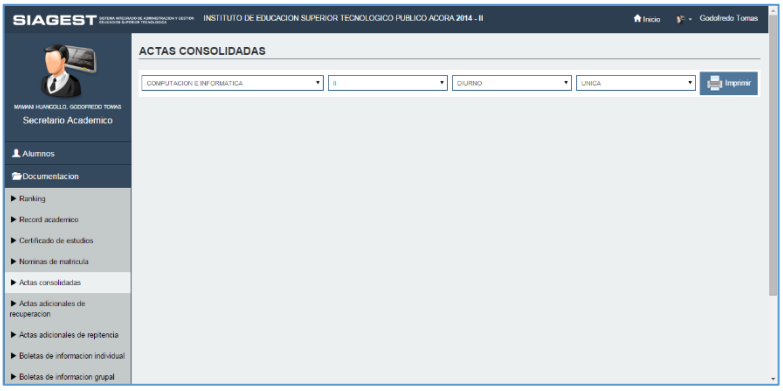

Figura 27. Formulario para reportar acta consolidada

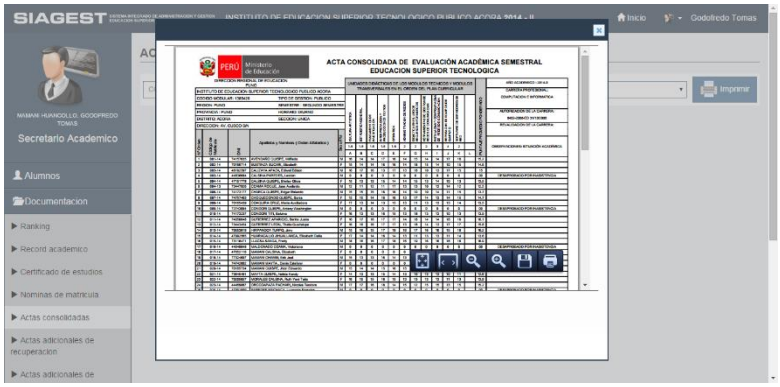

Figura 28. Reporte de acta consolidada

- Reportar Actas adicionales de recuperación.

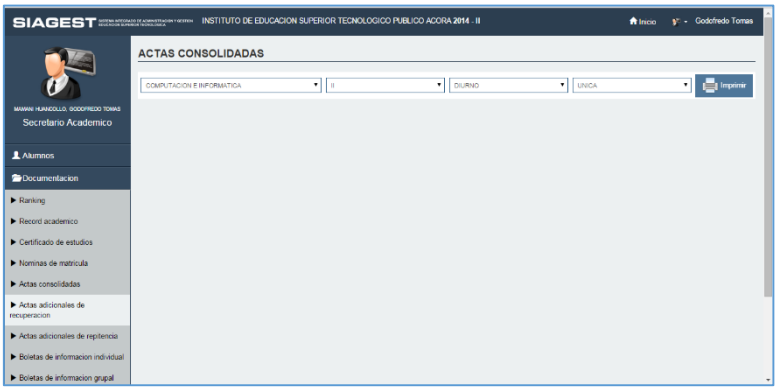

Figura 29. Reporte de actas adicionales de recuperación

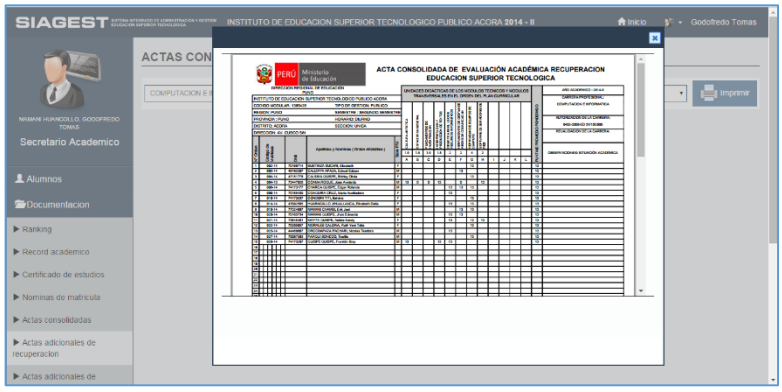

Figura 30. Reporte de actas adicionales de recuperación

- Reportar actas adicionales de repitencia

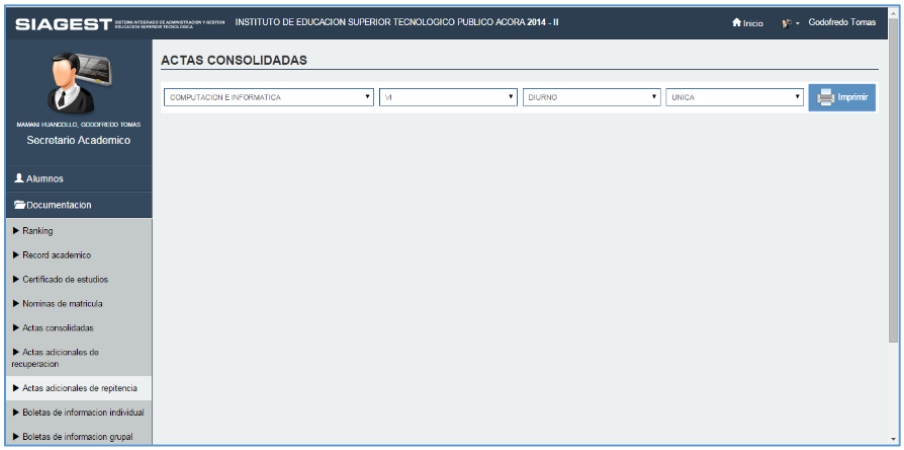

Figura 31. Reporte de actas adicionales de repitencia

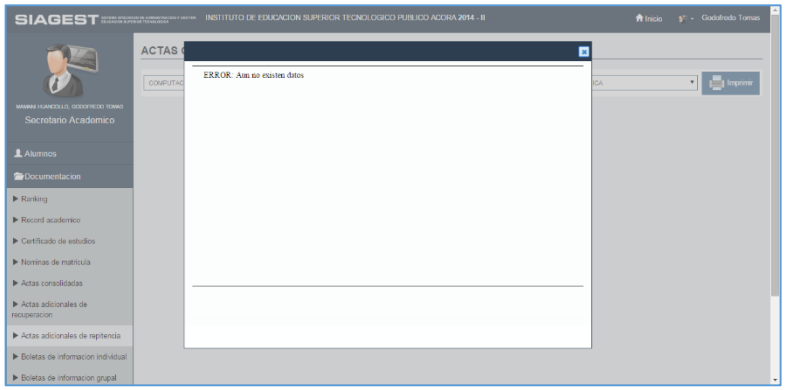

Figura 32. Reporte de actas adicionales de repitencia

- Reportar boletas de información individual.

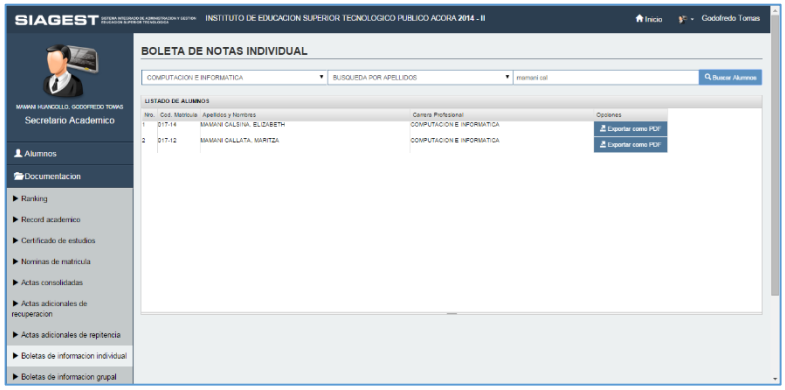

Figura 33. Formulario de búsqueda de alumno

Figura 34. Reporte de boleta de información individual

- Reportar boletas de información grupal.

Figura 35. Formulario para el reporte de boleta de información grupal

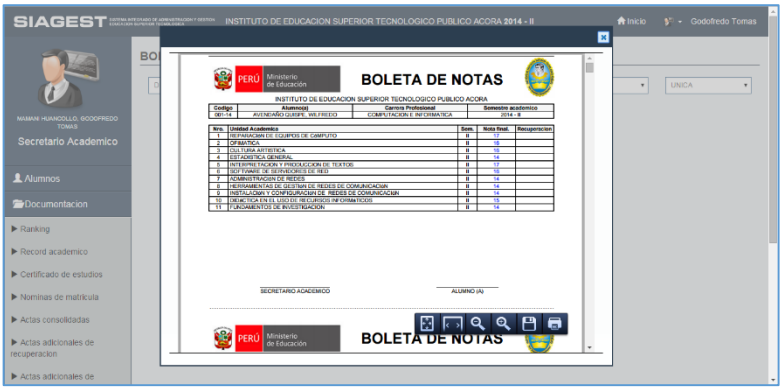

Figura 36. Reporte de boleta de información grupal

- Generar e imprimir accesos.

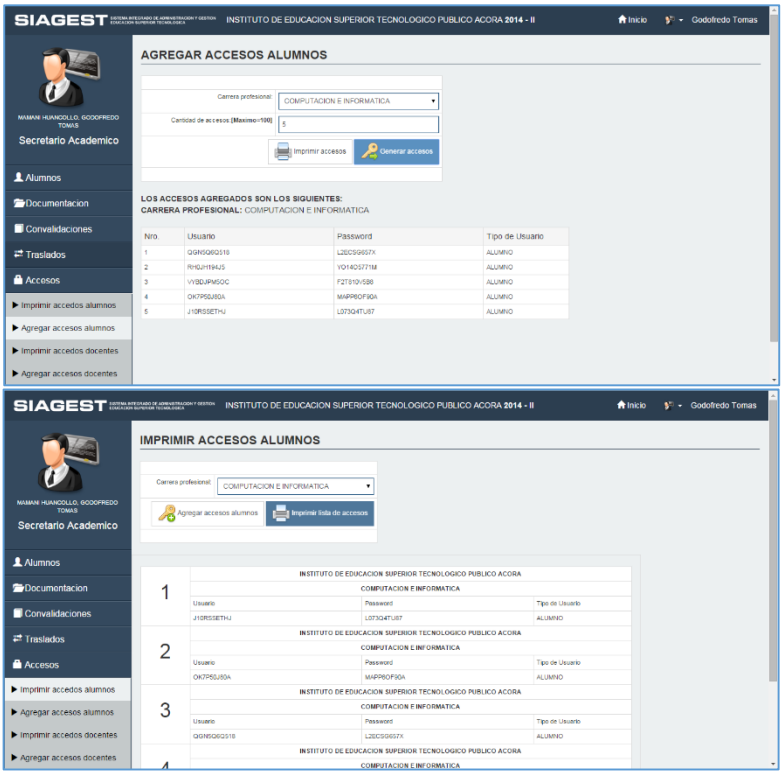

Figura 37. Generación e impresión de accesos alumnos

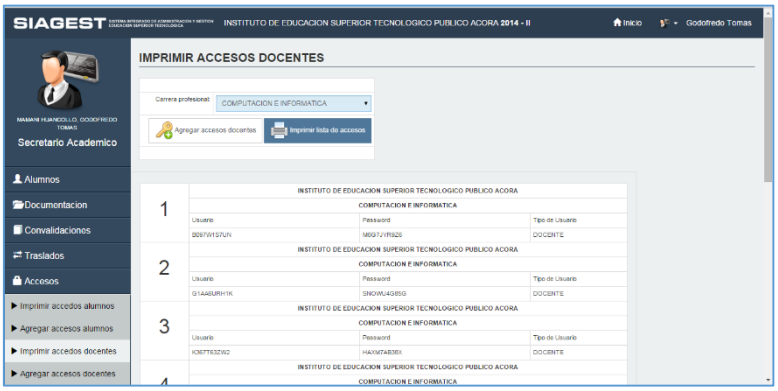

Figura 38. Generación e impresión de accesos docentes

- Configurar la institución.

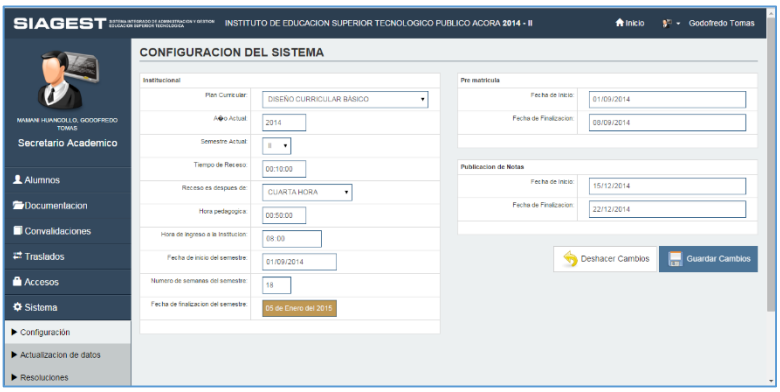

Figura 39. Configuración de la institución

- Actualizar datos de la institución.

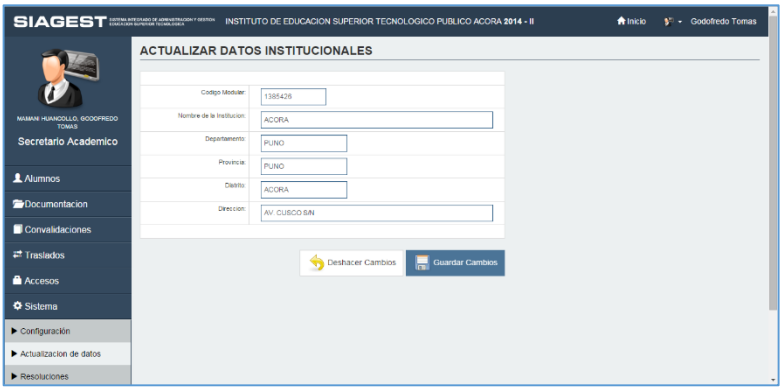

Figura 40. Actualización de datos de la institución

- Administrar Resoluciones institucionales.

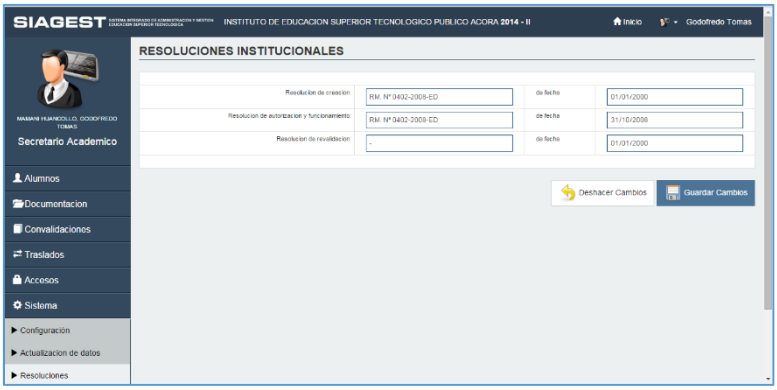

Figura 41. Administración de resoluciones

- Administrar cargos administrativos.

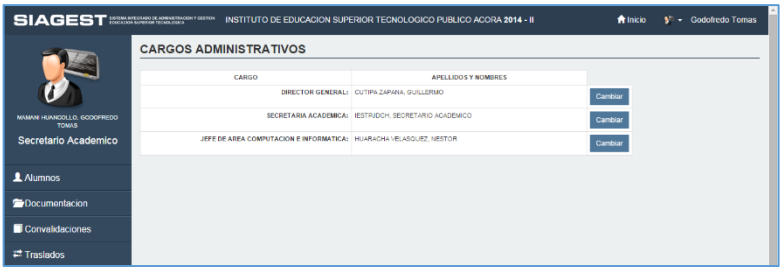

Figura 42 Administrar cargos administrativos

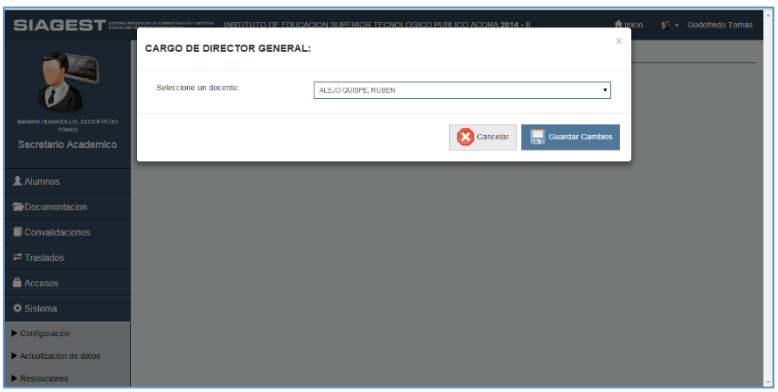

Figura 43. Cambiar un cargos administrativo

- Relación de docentes para imprimir.

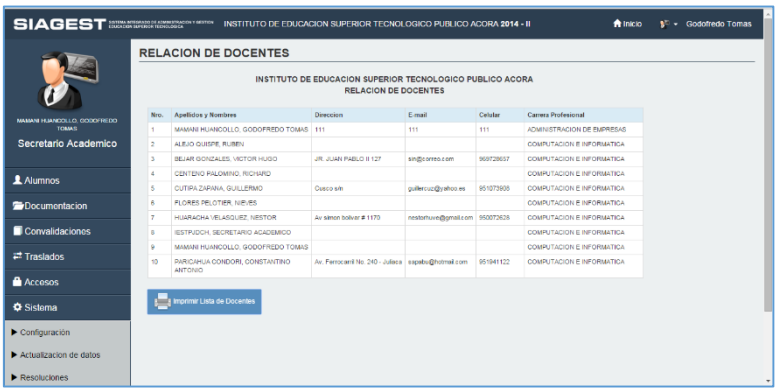

Figura 44. Relación de docentes

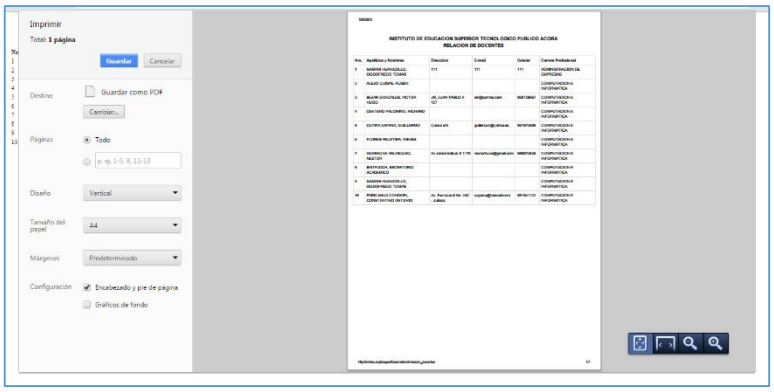

Figura 45. Vista preliminar de impresión de docentes

- Administrar el vínculo laboral.

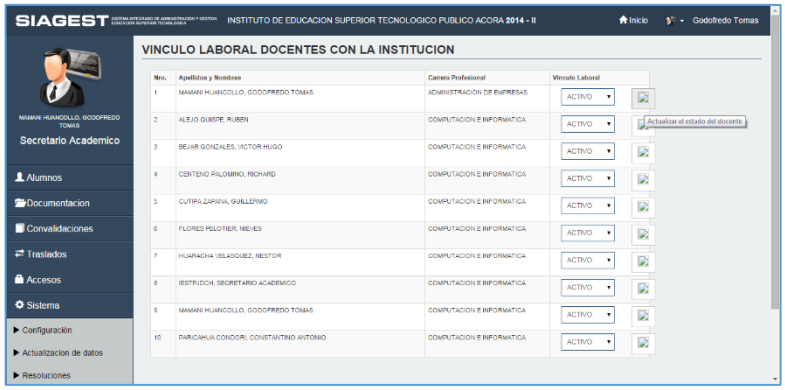

Figura 46. Administración del vínculo laboral

Los **usuarios docentes** tienen el permiso exclusivo de poder modificar las notas de los estudiantes mientras no apliquen la opción de publicación, cuando las notas se publican los usuarios estudiantes ya pueden visualizar sus notas con sus cuentas de usuario respectivas, los docentes para loguearse

lo pueden hacer desde cualquier punto con acceso a internet lo que resulta riesgoso ya que podría, por error, abandonar ese puesto de trabajo dejando un acceso logeado con su usuario de docente perjudicándose el mismo.

Las funciones que cumplen los docentes son los siguientes:

- Datos del docente.

Figura 47. Formulario para actualizar datos del docente

- Cambio de contraseña.

Figura 48. Formulario para cambiar contraseña del docente

- Listado de alumnos.

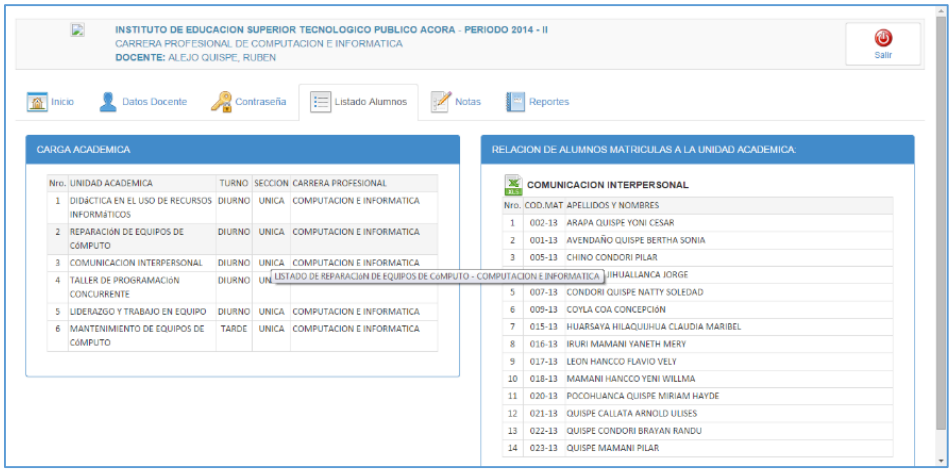

Figura 49. Listado de alumnos por unidad académica

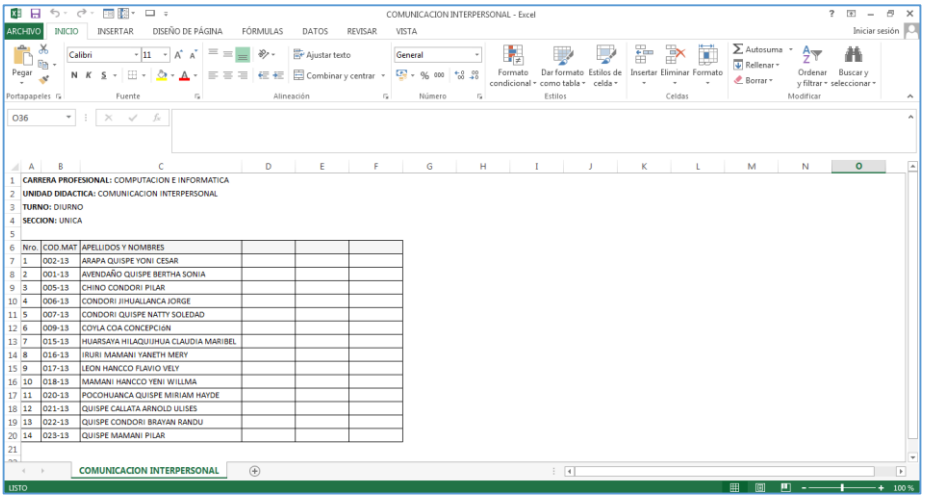

Figura 50. Listado de alumnos exportado a formato Excel

- Llenado de notas.

Figura 51. Listado de unidades académicas para llenado de notas

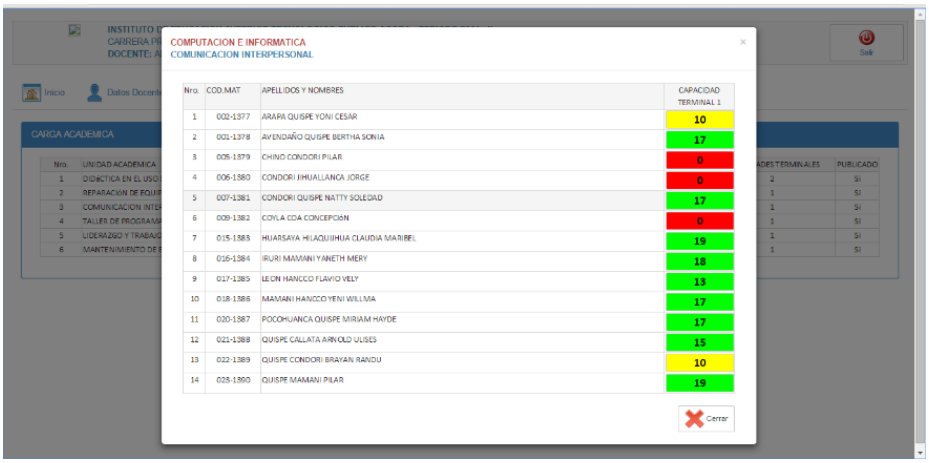

Figura 52. Llenado de notas

- Reportes del docente.

Figura 53. Listado de unidades académicas para realizar reportes

Figura 54 Reporte generado por el docente

Los usuarios que se encuentra en el grupo de jefes de área tienen permisos de lectura y escritura de datos según las funciones que la institución le brinda, para el acceso se loguean con su DNI precedido de un código proporcionado por la institución, su login lo pueden realizar desde cualquier punto con acceso a internet lo que resulta riesgoso ya que podría, por error, abandonar ese puesto de trabajo dejando un acceso logueado con su usuario de jefe de área perjudicándose el mismo.

Las funciones que cumplen los jefes de área son los siguientes:

- Distribución de carga académica.

Figura 55. Distribución de carga académica

Figura 56. Reporte PDF de la distribución de la carga académica

- Publicación de horarios para los distintos semestres.

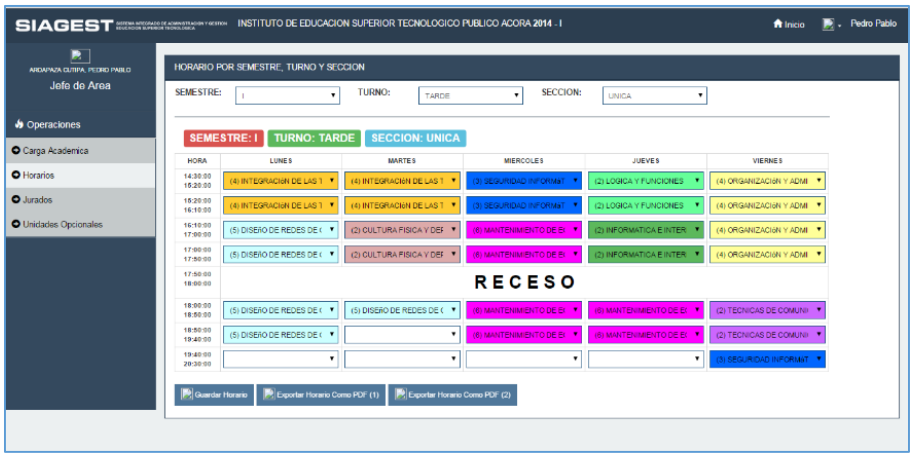

Figura 57. Creación de horario según semestre turno y sección

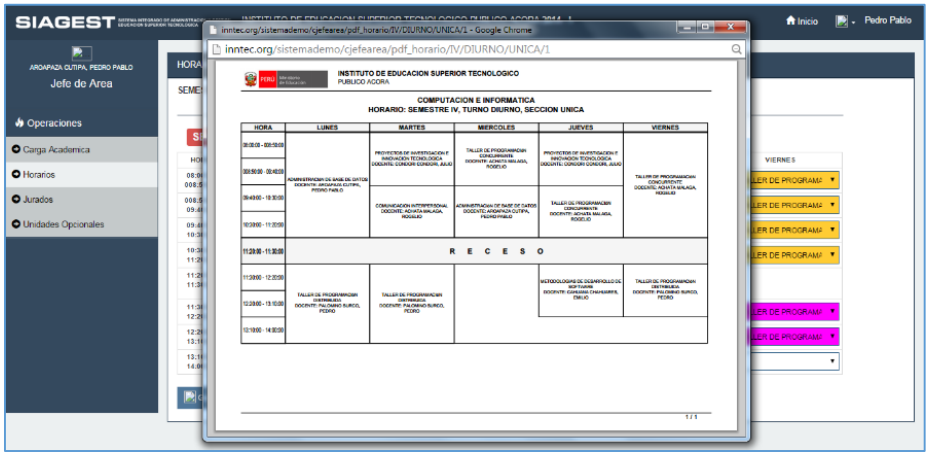

Figura 58. Reporte PDF del horario creado

- Programación y distribución de jurados para evaluaciones de recuperación.

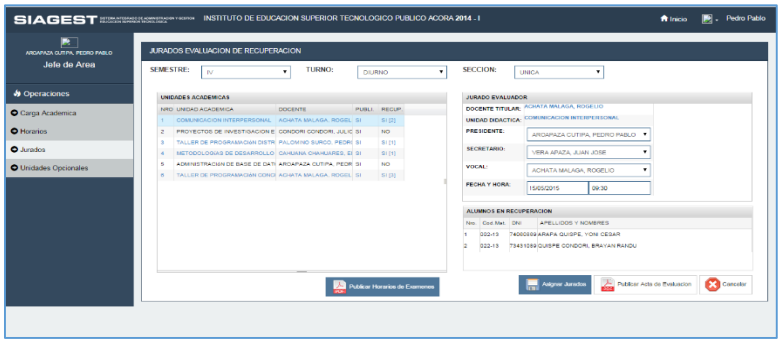

Figura 59. Asignamiento de jurados para recuperación

Figura 60. Reporte PDF del acata de evaluación de recuperación

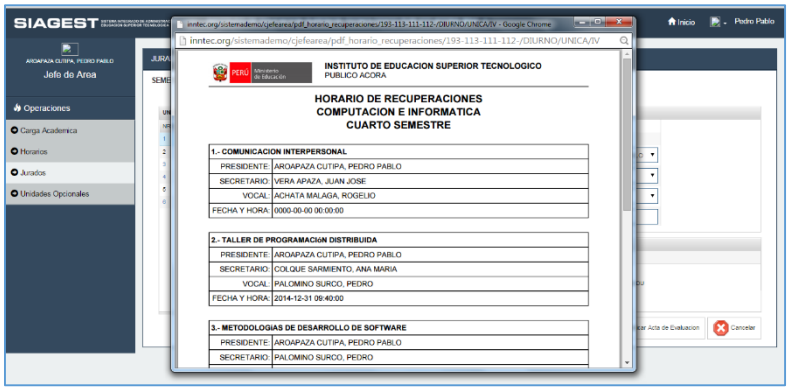

Figura 61. Publicación de recuperaciones

- Unidades académicas opcionales.

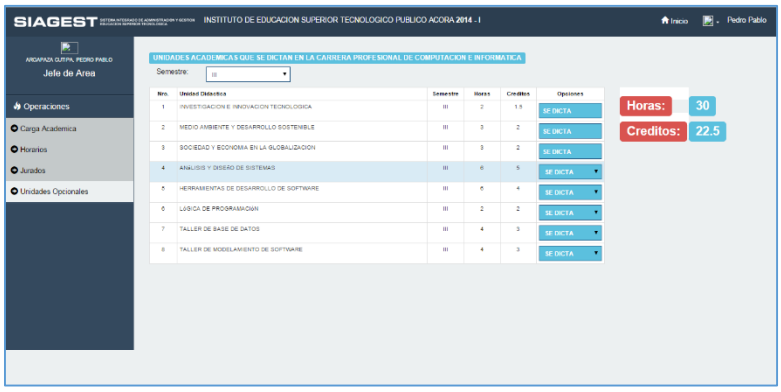

Figura 62. Asignación de unidades académicas opcionales

Los usuarios alumnos tienen el permiso le lectura mas no de escritura de datos, los alumnos para loguearse lo pueden hacer desde cualquier punto con acceso a internet lo que resulta riesgoso ya que podría, por error, abandonar ese puesto de trabajo dejando un acceso logeado con su usuario de alumnos perjudicándose el mismo ya que puede darse la posibilidad de que le cambien de contraseña o personas ajenas puedan ver sus notas.

Las funciones que cumplen los alumnos son los siguientes:

- Visualización de la programación de matrículas y labores académicas.

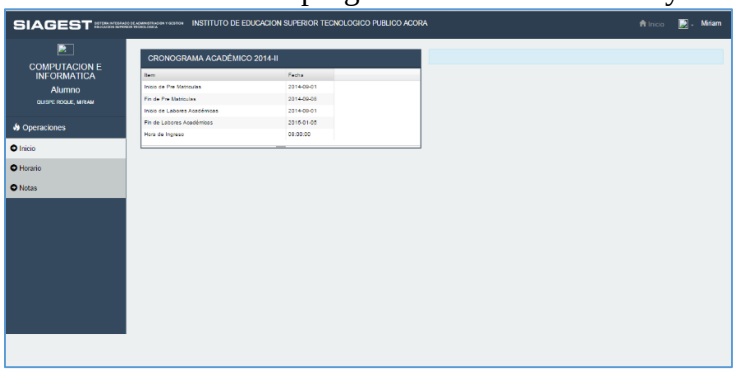

Figura 63. Visualización programación académica

- Visualización de horarios.

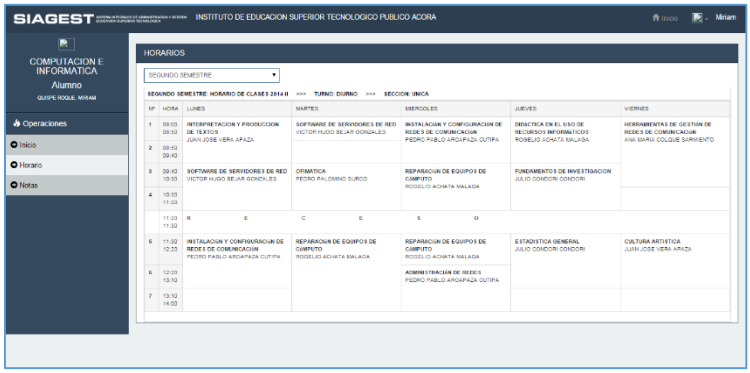

Figura 64. Visualización de horarios

- Visualización de sus notas.

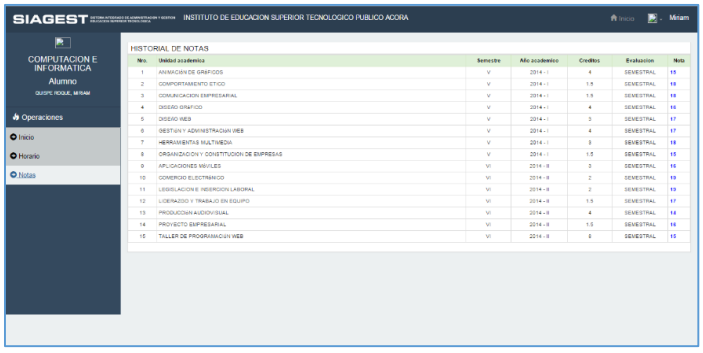

Figura 65. Visualización de notas

- Cambio de contraseña.

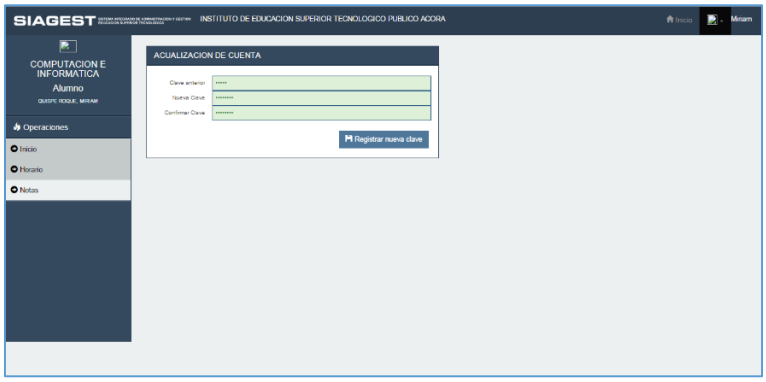

Figura 66. Cambio de contraseña

- Actualización de datos.

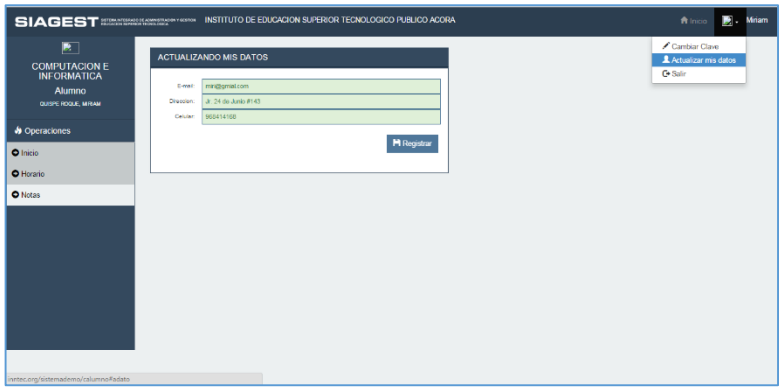

Figura 67. Actualización de datos

4.1.1.2 Autenticación

En la pantalla de login del sistema de información se piden los siguientes datos:

- Nombre de usuario (a completar por el usuario).
- Password (a completar por el usuario).

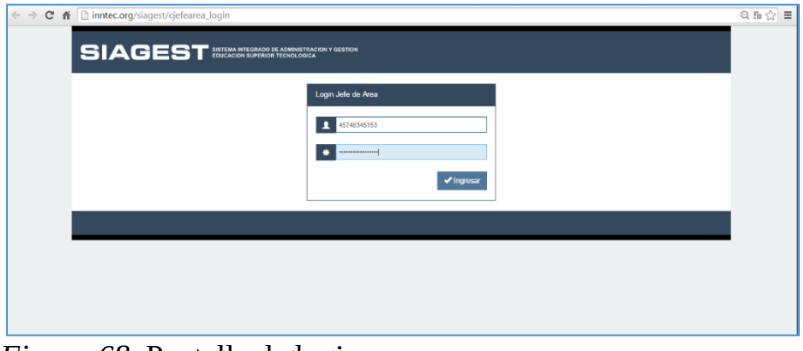

Figura 68. Pantalla de login

Cuando el usuario ingresa su password al sistema aparecen puntos negros en lugar de mostrar el dato que está siendo ingresado, una vez que un usuario se ha logrado loguearse al sistema, aparece en la pantalla el nombre del usuario que se ha logueado en el sistema.

Existe una aplicación de importante y significativa sensibilidad con la cual es posible gestionar los datos de los usuarios, incluidos sus permisos y contraseñas. Esta aplicación solo puede ser ejecutada si el usuario logeado es el proveedor del sistema, a través de un servicio que se encuentra en su hosting y dominio, ya que no hay íconos de acceso directo desde ninguna terminal. Los datos de autenticación de los usuarios del sistema de la Institución se almacenan en el servidor de aplicaciones Linux, en un archivo de texto plano, sin ningún control de acceso (con encriptación y password de acceso). Este archivo es administrado por el proveedor del sistema, ya que forma parte del sistema de archivos indexados de la institución.

Además, estos datos son transferidos, desde la terminal que se está logueando hasta el servidor, en formato de texto plano.

Dentro de la Institución no se usa ningún tipo de firma digital, ni para mensajes internos ni para los externos ya que las directivas de importancia no son enviadas vía mail.

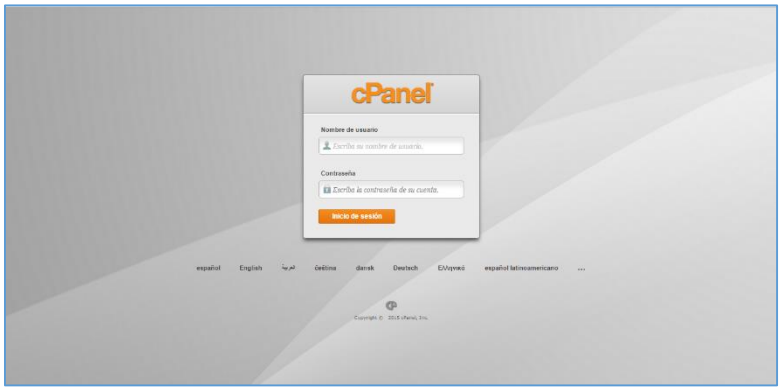

Figura 69. Login para el proveedor del sistema

En cuanto a la configuración de las estaciones de trabajo, no hay ningún control de acceso a sus sistemas BIOS, de manera que al momento del

encendido de la máquina cualquier persona podría modificar sus opciones de configuración.

4.1.1.3 Passwords

a. Generación

Los password que existen en la institución son generados en forma automática por el sistema.

Cuando se da de alta un empleado en el sistema, su password se inicializa con el número de su DNI precedido de un código que brinda el sistema, advirtiéndole al usuario que lo cambie, pero sin realizar ningún control sobre la modificación del mismo.

b. Cambios

Los cambios en los password los hacen los usuarios luego de haberse logueado, a través un botón que muestra la opción para su modificación y de una pantalla de cambio de contraseña. Aunque generalmente los password no son actualizados por los usuarios, permaneciendo iguales por largos períodos de tiempo.

No se controla si el usuario utiliza siempre el mismo password, simulando cambiarlo pero ingresando nuevamente la clave que ha estado usando hasta ahora.

Si un usuario olvida su password, debe de comunicarse con el proveedor del sistema, el cual se reestablecerá (con el sistema de administración general cpanel) la clave del usuario al de su DNI y el código autogenerado por el sistema.

4.1.2 Seguridad en las comunicaciones

Objetivo de auditoria: Durante la Auditoría Informática se deberá evaluar la seguridad de las comunicaciones, los datos transmitidos, los dispositivos usados durante la transmisión, la documentación necesaria para la realización eficiente e ininterrumpida de esta transmisión, y los sistemas usados para la transmisión de

datos de un entorno a otro, comprobando el cumplimiento de las normas de seguridad de la información.

4.1.2.1 Topología de red

Componentes de la Red.

La red informática de la institución se compone del siguiente equipamiento:

35 PCs. Distribuidas en dos centros de cómputo de la institución

- 01 receptor inalámbrico de internet.
- Cables UTP Cat. 5e.
- 02 Switch Satra de 48 puertos c/u.
- 01 Servidor proxy.
- 02 Laptop.

Figura 70. Alumnos en el centro de Cómputo 01

Figura 71. Centro de cómputo 02 – panorámico

Figura 72. Centro de computo 02

Descripcion De La Red.

Internet WiFi. Existe una conexión WiFi que es emitida desde el centro poblado de salcedo y recibida por un receptor que se encuentra en el techo del pabellón donde se encuentran las oficinas administrativas y los centros de cómputo de la institución.

Figura 73. Alumnos conectándose al Interne WIFI

Figura 74. Alumnos conectados a la red WIFI fuera de los salones de clase

Servidor Proxy. El servidor proxy se encarga de bloquear algunas páginas de acceso prohibido, redes sociales, youtube, controla las descargas y páginas de descargas como megaupload.

UTP en conexiones internas. La totalidad del tendido del cableado estructurado horizontal en la institución se realizó con cable UTP Cat 5e.

Figura 75. Switch conectado con UTP

Switch. Los switch conectan todas las 35 PCs comprendidas en los dos laboratorios de cómputo, así como las laptop de las oficinas administrativas.

Puntos de consulta para alumnos. Las 35 PCs de ambos centros de cómputo son los terminales para la consulta de notas de los alumnos, así como también son los puntos de acceso para los docentes y jefes de área académica puedan realizar sus tareas dentro del sistema. En los terminales se encuentra un acceso para el sistema donde los usuarios pueden loguearse sin ningún problema.

4.1.2.2 Conexiones externas

Servidor de internet

Para la **conexión a internet** se utiliza un servidor Proxy de Linux llamado Squid, ubicado en el servidor de Internet. Su salida al exterior es a través de una conexión WiFi, suministrada por un ISP. Este Proxy se configuró de manera estricta, de forma que solo tiene conexión al exterior un rango de direcciones IP definido por la Dirección General. En el servidor Proxy se seleccionaron las direcciones IP de las laptop de los alumnos que pueden salir al exterior, de esta manera se controla el acceso a Internet. Este Proxy es el que proporciona de acceso a Internet al resto de las alumnos a través de los enlaces radiales.

Como conexión de respaldo a Internet se puede utilizar una conexión vía módem. Actualmente no existe algún módem instalado en el servidor, para su protección física, pero puede ser instalado y configurado rápidamente ante cualquier contingencia con la conexión de WiFi.

Figura 76. Servidor de la institución

Servidor de hosting

El servidor de hosting se eligió según el precio y los servicios ofrecidos. No se ofrece ninguna medida de seguridad ni política de respaldo en caso de problemas, pero no se han registrado problemas hasta el momento.

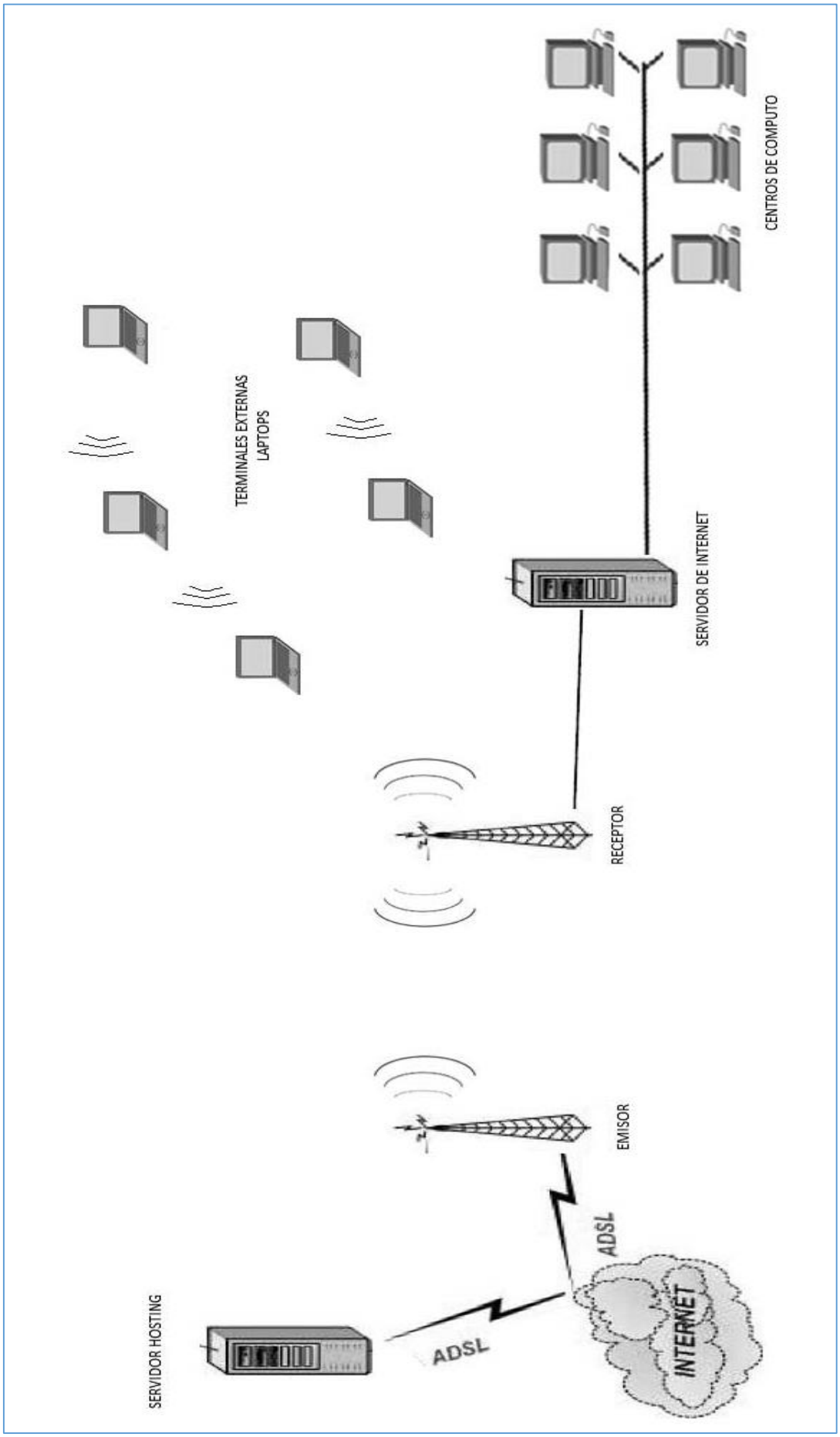

Figura 77. Grafico Topológico De La Red

4.1.2.3 Configuración lógica de la red

Interoperatividad Windows – Linux

Los recursos de Linux se comparten en la red de Windows usando una aplicación llamada Apache. Con esta aplicación, una porción del disco del servidor de aplicaciones donde se encuentra el sistema, se encuentra compartida con la red de Windows. Esto hace posible el entendimiento entre Windows y Linux, permitiendo a los usuarios de Windows acceder a datos que se encuentren en el sector compartido del servidor hosting - Linux, a través del Explorador de Windows.

Apache mediante el sistema de información tiene la capacidad de realizar autenticación, administrar perfiles, y demás opciones de seguridad de los recursos compartidos, donde se le establece un nivel de seguridad determinado a cada uno de los recursos de la red.

Recursos compartidos

El entorno de red de cada uno de los usuarios está configurado para que le usuario no vea toda la red, sino solo una parte de la misma. Pero no hay ninguna medida tomada para que un usuario no comparta sus datos con otro usuario.

En la Institución, la configuración de esta aplicación no permite que haya visibilidad a las carpetas compartidas de los servidores, debido a que están en el área compartida del disco con la aplicación Apache, pero no disponibles para los usuarios en el Explorador de Windows.

Ninguno de los equipos comparte sus archivos, a excepción de los siguientes:

- En el servidor de Internet se comparten dos carpetas. Una es la utilizada para almacenar las actualizaciones del antivirus y los instaladores más utilizados, y la otra es la que emplea la aplicación que sincroniza la fecha y hora de las PCs de la red.

- En el servidor de hosting se comparte el sistema de información donde los usuarios de acceden con su login respectivo.

4.1.2.4 Antivirus

En la Institución existen problemas con virus, a excepción de las laptops que de fábrica vinieron instaladas predeterminadamente el antivirus Norton, las demás PCs con Windows infectadas con el virus K-Lez, pero este virus no afectó a los servidores Linux. Esta infección generó gran tráfico de red y congestionó la líneas y puso lentas las maquinas, pero pudieron erradicarse con el uso del antivirus ESET NOD 32 6.0.

Herramientas

En la institución disponen de una versión del Antivirus ESET NOD 6.0, de manera que en las PCs hay una versión cliente de este antivirus. En el servidor de Internet no se instaló ningún antivirus debido a que el sistema operativo es Linux. El antivirus está ejecutándose continuamente y controlan la recepción y el envío de mail, UBS, CDs, y otros medios extraíbles, tanto en la información que los estudiantes, docentes y personal administrativo introducen.

Actualización

De Internet se actualizan las listas de virus del ESET NOD 32 a través de un script interno del antivirus. Este script, al ejecutarse y bajar las actualizaciones, analizan automáticamente los medios extraíbles que se introducen en los diferentes terminales. No se hacen chequeos ocasionales para ver si se han actualizado los antivirus.

Escaneo de virus

No se hacen escaneos periódicos buscando virus en los servidores ni en las PCs. No hay ninguna frecuencia para realizar este procedimiento, ni se denominó a ningún responsable. En algunas máquinas (en las que han tenido problemas frecuentes con virus), cuando el equipo se inicia, entonces comienza un escaneo del automático antes del inicio de Windows.

4.1.3 Seguridad de las aplicaciones

Objetivo de auditoría: La auditoría Informática deberá evaluar la seguridad de las aplicaciones utilizadas en la Institución, la consistencia de sus datos de entrada y la exactitud de sus datos de salida, la integridad de las bases de datos y la existencia y el uso de la documentación necesaria para su funcionamiento, de acuerdo a los estándares propuestos.

4.1.3.1 Software

En la Institución hay un servidor, con sistema operativo Linux Centos, como servidor de internet. Se eligió este sistema operativo por las siguientes razones:

- Porque necesitaban migrar a un sistema con entorno gráfico.
- Por el bajo costo (y la diferencia de precio con Windows NT),
- Porque estaban utilizando un sistema operativo (C-Tos) que era muy similar al Unix y la migración resultaba fácil,
- Por la confiabilidad,
- Por la compatibilidad que tiene con Windows (en el explorador de Windows se pueden ver las carpetas compartidas de Linux por el uso de un emulador),
- Por el buen control de acceso y la buena generación de logs de auditoria.
- Por la posibilidad de conseguir actualizaciones,
- Por el software de aplicación gratis,
- Por una experiencia mala con Windows, y una buena experiencia con UNIX,
- Por buenos consejos de profesionales capacitados de la UTN.

El 80% de las PCs usan el sistema operativo Windows Seven, en el resto de ellas hay Windows XP. No usan software comprado, a excepción de los sistemas: Microsoft Office, StarOffice, y demás utilitarios, y sistemas propietarios de las fábricas.

4.1.3.2 Seguridad de base de datos

El sistema de información utiliza PHPMyAdmin como gestor de base de datos.

El único autorizado a ingresar a la base de datos es el proveedor del sistema, mediante un acceso que el solo conoce.

No se realizan controles de acceso lógico, a las tablas donde están almacenados los datos, a lo que se agregan los controles de seguridad física del servidor.

El sistema informático que administra la base de datos disponen de recursos suficientes para su funcionamiento, ya que aproximadamente.

Cuando algún usuario elimina registros de una base de datos, éstos no se borran físicamente sino que son marcados como borrados. De esta forma siempre permanecen los registros de las transacciones realizadas.

4.1.3.3 Control de aplicaciones en Psc

No hay estándares definidos, no hay procedimientos a seguir ni tampoco documentación respecto a la instalación y actualización de la configuración de las PCs. Solo hay una instalación básica de alguna versión del Windows, Internet Explorer, ESET NOD 32.

En el caso de que una PC presente errores en su configuración, se utilizan herramientas de reparación de errores, como el Norton Disk Doctor, con el fin de evitar la reinstalación total del sistema y así causar una pérdida innecesaria de tiempo.

Tampoco se realizan actualizaciones de los programas instalados, como el Internet Explorer, Google Chrome y Microsoft Office. No se buscan Service Packs ni nuevas versiones. La política de actualización de

programas que se lleva a cabo permite actualizar los programas solo si es necesario debido a algún mal funcionamiento o nuevo requerimiento, lo que facilita la continuidad de los programas.

Las única versión que se actualiza y quedan documentadas es el sistema informático académico. Estas versiones se actualizan mediante internet, lo que evita hacer el control en cada una de las máquinas.

Solamente los administradores del centro de cómputos son los encargados de las instalaciones en las PCs, aunque para los usuarios no existen restricciones con respecto a la instalación de programas. Pueden bajar de la web cualquier aplicación e instalarla en su PC sin ningún control sobre las licencias ni autorización previa. Esto se debe a que, para controlar problemas de licencias, virus o programas no permitidos, no hay ninguna herramienta en uso ni se realizan auditorías internas periódicas. En una sola oportunidad fue necesario el registro on line de un aplicativo de emisión de mails que solicitó la gerencia.

Cuando se hace un cambio en la configuración del servidor, se guardan copias de las configuraciones anterior y posterior al cambio, pero no se documentan los cambios que se realizan ni la fecha de las modificaciones.

4.1.4 Seguridad física

Objetivo de auditoría: se evaluará que el centro de cómputos, los equipos, los dispositivos, los medios de almacenamientos y las personas que conforman el sistema informático de La institución cumplan con las medidas necesarias en lo relativo a la infraestructura física y al mantenimiento de la seguridad de los recursos de la organización.

4.1.4.1 Equipamiento

Características del servidor de internet

En la institución existe un servidor de internet (servidor proxy) que es un Servidor Hewlett Packard LC 2200, donado en el año 2010, con las siguientes características.

- 2 Procesadores (redundantes) Pentium III 550 MHz
- 2 Fuentes (redundantes)
- 2 Placas de red (redundantes)
- 4 GB de memoria RAM.
- 3 discos con tecnología SCSI con 100 GB de capacidad cada uno.
- Sistema UPS de suministro alternativo de energía.
- Generador de energía eléctrica.

Características de las PCs

La institución en su totalidad posee alrededor de 35 PCs, distribuidas en los dos laboratorios.

20 máquinas que pertenecen al primer laboratorio las cuales son PCs Intel Pentium IV de 1GB de RAM, procesador de 800 GHz disco duro de 80GB. En el segundo laboratorio se cuentan con 15 PCs con procesador Intel Core Dos Duo de 2.2 Ghz, 3GB de RAM y 350 GB de Disco Duro.

La institución ha tomado la decisión de asegurar su red, debido al gran costo que implicaba contratar un mantenimiento tercerizado permanentemente.

4.1.4.2 Control de acceso físico a los centros de computo

En el momento de la instalación del centro de cómputos no se efectuó un análisis de costo-beneficio para determinar que controles de acceso físico sería necesario implementar.

Existe un circuito cerrado de cámaras de video. Este sistema no es exclusivo del centro de cómputos, ya que las cámaras están en toda el área administrativa de la de éstas cámaras apunta al centro de cómputos o a su puerta de ingreso.

La institución cuenta con personal encargado de laboratorios que se encargan de asegurar los ambientes mencionados; en horarios laborales se

ubican en el interior y exterior de la misma, y cuando se cierra la empresa solo quedan en el exterior, porque queda activado el sistema de alarma. No hay tarjetas magnéticas de entrada ni llaves cifradas en ningún sector de la institución.

4.1.4.3 Control de acceso a equipos

Todas las máquinas de la institución disponen de entradas USB y lectoras de CD, aunque el 90% de los usuarios no las necesita para el uso del sistema de información académico ya que el ingreso de datos está en la memoria de los usuarios. Solo algunas máquinas de administración y secretaria académica que necesitan entradas USB para utilizarlas como medio de transporte de información que es reportada a la Dirección General o entradas USB que son conectadas a impresoras para reportar los documentos que emite el sistema informático académico, deben utilizarlas como medios de entrada de datos, a pesar de que se está empezando a utilizar Internet para el intercambio de información.

Estos dispositivos están habilitados y no hay ningún control sobre ellos, no se hacen controles automáticos de virus ni se prohíbe el booteo desde estos dispositivos. Nunca hubo robo de datos usando medios externos, solo fue necesario hacer bloqueos de las impresoras para restringir los datos de salida del sistema, previniendo posibles fraudes.

Los switch de cada uno de los centros de cómputo, están abiertos al aire libre sin llave, donde inevitablemente el personal de limpieza o cualquier persona puedan desconectar las entradas, no tomando las medidas de precaución, debido a que hay bocas libres en estos dispositivos. Las llaves de todos los gabinetes están en el centro de cómputos

No se realizan controles periódicos sobre los dispositivos de hardware instalados en las PCs, de manera que alguien podría sacar o poner alguno. Una vez que se ha completado la instalación de algún equipo, el personal encargado de las PCs no realiza chequeos rutinarios o periódicos, solo revisa los equipos ante fallas en los mismos, o por un problema reportado por el usuario.

Los servidores del centro de cómputos no se apagan en horarios no laborales, permanecen prendidos las 24 horas del día, aunque durante la noche no se realizan trabajos, permanecen ociosos, debido a que no existen procedimientos en lote (El sistema de información académico se ejecutan online).

4.1.4.4 Dispositivos de soporte

En la institución se disponen de los siguientes dispositivos para soporte del equipamiento informático:

- Extintor: son equipos químicos, manuales y están instalados y adquiridos de una empresa externa, quienes deciden el lugar en que van a estar ubicados, el centro de cómputos cuenta con uno propio, ubicado en la habitación de los servidores.
- UPS: (Uninterruptible Power Supply) en el centro de cómputos hay un UPS que pueden mantener los servidores y las máquinas de desarrollo funcionando por 2 horas.

4.1.4.5 Estructura del edificio

Cuando se construyó el pabellón de la institución, no se tuvo en cuenta el diseño del centro de cómputos y sus condiciones de seguridad. Las paredes externas del centro de cómputos son poco elevadas (aproximadamente 2 mts.) y las ventanas tienen rejas soldadas y vidrios con cortinas que impiden la visibilidad desde el exterior del mismo.

En toda la institución hay vidrios y cortinas externas, que dividen los sectores del área administrativa, por lo que solo se ven los monitores desde el interior de cada área.

Figura 78. Instituto de Educación Superior Tecnológico Publico Acora

4.1.4.6 Cableado estructurado

La instalación del cableado fue realizada por los docentes de la institución conjuntamente con algunos alumnos, y se implementó un cableado estructurado, brindándole a la institución un trabajo de bajo costo, aunque el cableado estructurado se hizo utilizando canaletas de calidad regular que están ubicadas aproximadamente a un metro del piso, distanciando los cables eléctricos de los cables de red para garantizar una buena funcionalidad de la red, evitando así los campos magnéticos.

Estos cables no tienen bocas instaladas ni jacks con rocetas, pero sí están conectados al switch directamente sin la utilización de un Patch Panel. En algunas partes del cableado estructurado se pueden ver los cables que cuelgan debido a que con el tiempo se necesitaron más puntos y las canaletas que ya estaban instaladas no soportaban agregar más cables.

En todo el trayecto del cableado se tuvo en cuenta la distancia mínima necesaria entre cables para no provocar interferencias, daños o cortes. Además no hay distancias grandes recorridas con cables UTP.

En el switch hay una boca dedicada para cada máquina, y bocas de sobra por una posible ampliación de la red.

Para que no haya interferencias se utilizó cableado UTP categoría 5e, los cables en el switch están etiquetados de manera que se los puede identificar fácilmente.

4.1.5 Auditorias y revisiones

Objetivo de Auditoría: La auditoría Informática deberá evaluar las metodologías de control, auditorías internas y revisiones que se lleven a cabo en forma periódica, con el fin de encontrar debilidades y proponer mejoras, con base en las normativas que asesoran en el buen desempeño de la auditoría interna en una Organización.

4.1.5.1 Chequeos del sistema

Generación y Administración de log

El sistema no genera log, ni gráficos de estos mismos para informar del estado del sistema, los chequeos de log tampoco se generan de manera manual no se generan reportes avisando a los usuarios del sistema sobre cambios realizados sobre su la base de datos.

Log de Servidores

El kernel de Linux monitoriza los servidores generando entre otros, logs sobre:

- Los servicios de mail,
- Servicios de red,
- Configuración,
- Utilización del CPU,
- Reinicio de servidores.

4.1.5.2 Responsabilidad del encargado de seguridad

El encargado del centro de cómputos:

- No Administra, ni desarrolla e implementa los procedimientos de auditoría y revisión.

- No Monitoriza y reacciona a los avisos (warnings) y reportes.
- No Realiza chequeos aleatorios para verificar el cumplimiento de los requerimientos y procedimientos de seguridad.
- No Revisa los reportes de auditorías o logs cuando es advertido de anomalías.
- El encargado del mantenimiento de los servidores determina qué logs se generan, qué eventos de seguridad se auditan y qué datos se recogen. Además se encarga de buscar nuevas herramientas que faciliten la auditoría.

4.1.5.3 Auditoria de control de acceso

Control de Acceso al Log

Los logs se almacenan en el servidor de Internet, por lo que cuentan con el control de acceso físico al servidor, pero no hay ningún control de acceso lógico a la base de datos del sistema de información académica.

Modificación de Datos

El sistema informático académico no genera logs indicando qué datos se han modificado y en que momento y estos no son analizados por encargados en la institución. No existen logs sobre la mayoría de los movimientos de los usuarios en el sistema informático de la institución.

Cambios de Password

No se generan logs cuando un usuario modifica su password, no se guardan las contraseñas anteriores (para evitar la repetición), no se determina que aplicación se ha usado para realizar el cambio ni, en caso que el cambio resulte fallido, el motivo del fallo.

Login Fallido

Tanto el login exitoso como el fallido no generan un log y n se puede saber si el motivo del fallo de login o si hubieron login exitosos, como por ejemplo si falló porque el password estaba mal, porque el usuario no existe,

o porque tuvo dos intentos errados. Solo se identifica que hubo un error de conexión.

4.2 Informe de debilidades y recomendaciones

4.2.1 Seguridad lógica

4.2.1.1 Identificación de usuarios

Debilidad

Cuando el sistema genera los password estos no cambiados por la mayoría de los usuarios.

Efectos

Esto podría generar fuga de información y mala manipulación de los datos en el sistema y que otros usuarios puedan ver información confidencial de otros usuarios.

Recomendaciones

Se recomienda generar un script para bloquear al usuario si este no cambio su contraseña en un mes desde el primer logueo.

Debilidad

Usuarios inescrupulosos pueden generar script para lograr loguearse al sistema con una cantidad indefinida de logueos.

Efectos

Infiltración de usuarios que no tienen relación con el sistema, dando como resultado pérdida o filtración de información no debida ni permitida.

Recomendaciones

Se recomienda bloquear la PC desde donde se intentó acceder por lo menos una hora luego de tres intento de login, si el usuario se encuentra registrado en la base de datos y no puede loguearse por las de cinco intentos bloquear la cuenta.

Debilidad

No se lleva a cabo ninguna revisión periódica ni control sobre el buen funcionamiento de las cuentas de los usuarios, ni sobre los permisos que tienen asignados.

Efectos

Usuarios descontentos al querer acceder al sistema y revisar la información que les interesa.

Recomendaciones

Llevar cabo mensualmente un reporte sobre el control de funcionamiento de las cuentas de usuarios.

Debilidad

El tiempo de sesión de los usuarios es indeterminado.

Efectos.

Si una sesión se deja abierta cualquier persona se puede filtrar en el sistema y causar daños sobre la información de la institución.

Recomendaciones

Las sesiones de usuario se deben destruir luego de pasado media hora de inactividad.

4.2.1.2 Passwords

No se encontraron debilidades

4.2.2 Seguridad en las comunicaciones

4.2.2.1 Topología de la red y conexiones externas

Debilidad

En la topología de la red se ha notado que las conexiones inalámbricas están libres para las laptops debido a una mala configuración del servidor de internet.

Efectos

La línea se entrecorta de momento en momento debido a que los usuarios acceden a páginas que consumen bastante el ancho de banda.

Recomendaciones

Configurar adecuadamente el servidor de internet para bloquear el acceso libre a internet dentro de la institución y así solucionar el problema de la conexión a internet.

4.2.2.2 Configuración lógica de la red

No existe ninguna debilidad.

4.2.2.3 Antivirus

Debilidad

Deficiencia en el antivirus en poder encontrar código malicioso.

Efectos

Maquinas infectadas con virus que no es perceptible por el hombre causando daños a los terminales poniendo lentas las PCs, usuarios inconformes al momento de utilizar el sistema informático académico.

Recomendaciones

Se recomienda actualizar la versión del antivirus ESET NOD 32 6.0 a la versión ESET NOD 32 8.0.

4.2.3 Seguridad de base de datos

4.2.3.1 Seguridad de base de datos

Debilidad

No existen log para identificar los cambios que se realizan en la base de datos impidiendo hacer una auditoría.

Efectos

Desconocimiento de los cambios físicos en la base de datos.

Recomendaciones

Se recomienda sostener una reunión con el proveedor del sistema informático con la finalidad de implementar log que permitan realizar seguimientos sobre la base de datos.

4.2.3.2 Control de aplicaciones de Pcs

No se encontraron debilidades.

4.2.4 Seguridad física

4.2.4.1 Control de acceso físico a los centros de computo

Debilidad

No hay control de acceso físico al centro de cómputos, ya que ninguna de las cámaras del circuito cerrado de video lo apunta a él o a su puerta de ingreso.

Efectos

Al no haber un control de acceso especial en el centro de cómputos, cualquier persona que tenga acceso al área de administración y ante una distracción del personal, puede ingresar en él, con todo el riesgo que esto implica, debido a la sensibilidad crítica de los datos y activos que allí se encuentran.

Recomendación

Sería conveniente que el área del centro de cómputos, donde se encuentran los servidores, el switch central y demás equipamiento crítico tenga una medida de seguridad extra, a través de la cual solo se permita el acceso a los administradores. Esto podría implementarse con una llave, ya que no implica mucho gasto y pueden darse copias solo al personal necesario. O, en reemplazo de esta medida, puede agregarse una cámara extra de video

que grabe el interior del centro de cómputos, o modificar la orientación de alguna existente hacia la puerta de ingreso al mismo.

4.2.4.2 Dispositivo de soporte

Debilidad

No existe una alarma en la institución que se activa en los horarios donde no hay atención a los usuarios, generalmente de noche cuando se cierra la institución.

Efectos

Posibles intromisiones de personal no autorizado en los centros de cómputo y oficinas administrativas, perjudicando así la utilización del sistema informático académico.

Recomendaciones

Se recomienda contactarse con una empresa para poder instalar sistemas de alarma con sensores de movimiento, sensores de pánico entre otros.

4.2.4.3 Estructura del edificio

No se hallaron debilidades significativas con respecto a este tema.

4.2.4.4 Cableado estructurado

Debilidad.

El cableado estructurado con que cuenta la institución no está implementado con los estándares de calidad que exigen las normas, en algunos casos hemos visto cables de distintas categorías.

Efectos.

El internet se vuelve lento mala conectividad entre dispositivos.

Recomendaciones

Hacer un recableado estructurado de toda la red.

4.2.5 Auditorias y revisiones

4.2.5.1 Chequeos del sistema

Debilidad

El sistema no genera log, ni gráficos de estos mismos para informar del estado del sistema, los chequeos de log tampoco se generan de manera manual no se generan reportes avisando a los usuarios del sistema sobre cambios realizados sobre su la base de datos.

Efectos

Se desconoce de la actividad física que se da sobre la base de datos.

Recomendaciones

Coordinar con el proveedor del sistema para realizar las implementaciones de los log en el sistema.

4.2.5.2 Responsabilidades del encargado de seguridad

No se hallaron debilidades significativas con respecto a este tema.

4.2.5.3 Auditoria de control de acceso

Debilidad

El sistema informático académico no genera logs indicando qué datos se han modificado y en qué momento y estos no son analizados por encargados en la institución. No existen logs sobre la mayoría de los movimientos de los usuarios en el sistema informático de la institución.

Efectos

Falta de información sobre la actividad de las modificaciones que se realizan sobre la base de datos.

Recomendaciones

Coordinar con el proveedor del sistema para realizar las implementaciones de los log en el sistema.

CONCLUSIONES

- Con la evaluación de sistema se pudo determinar que los accesos de los usuarios al sistema deben ser más restringidos, especialmente los accesos de los docentes, jefes de área y aún más restringido los secretarios académicos.
- La seguridad lógica nos indica que se debe de realizar las configuraciones necesarias a los equipos necesarios con la finalidad de optimizar mejor los procesos de acceso al sistema sin poner en riesgo el sistema académico, estando libre de virus con una buena conexión a internet.
- Levantar los requerimientos que se van presentando con el uso del sistema académico de la institución, para su pronta solución y continuidad con el ciclo de vida del software.
- Instalar sistemas de alarma con sensores de movimiento, sensores de pánico entre otros.
- Es necesario realizar un recableado estructurado de toda la red, empleando como mínimo la categoría 5e para el cableado de toda la red.
- Las aplicaciones que se vayan a instalar en las maquinas deben de estar protegidas por un buen antivirus actualizado, con la necesidad de comprar la licencia de ESET NOD 32 Antivirus, y de ser posible emplear el software DeepFrezer para mantener las maquinas en un estado determinado.
- Implementar el LOG del sistema para identificar las modificaciones inserciones y escaneo de datos dentro de la base de datos para poder tomar decisiones.

RECOMENDACIONES

- Se recomienda controlar mejor el acceso de los usuarios controlando el punto de acceso la hora y los intentos de login de un usuario, obteniendo la dirección física de la PC desde donde se intentó ingresar, guardando esta información en una base de datos que sirva para la toma de decisiones en la institución.

- Realizar configuraciones al servidor de internet para controlar mejor el acceso de cuentas usuario a la institución para optimizar el acceso a internet.

- Comprar la licencia del antivirus ESET NOD 32 8.0 previniendo así el contagio de virus que pueda dañar los puntos de acceso de internet dentro de la institución y así no generar la necesidad de buscar otros puntos de acceso o por lo menos no generar muchos puntos de acceso.

- Se recomienda sostener una reunión con el proveedor del sistema informático con la finalidad de implementar log que permitan realizar seguimientos sobre la base de datos.

- Sería conveniente que el área del centro de cómputos, donde se encuentran los servidores, el switch central y demás equipamiento crítico tenga una medida de seguridad extra, a través de la cual solo se permita el acceso a los administradores. Esto podría implementarse con una llave, ya que no implica mucho gasto y pueden darse copias solo al personal necesario, o en reemplazo de esta medida, puede agregarse una cámara extra de video que grabe el interior del centro de cómputos, o modificar la orientación de alguna existente hacia la puerta de ingreso al mismo.

- Realizar recableado estructurado de toda la red.

- Coordinar con el proveedor del sistema para realizar las implementaciones de los log en el sistema.

BIBLIOGRAFÍA

Cabarcas Gómez, J. A. (26 de Diciembre de 2013). *Glosario de términos importantes de Programación y Redes.* Available from: http://www.cpxall.com/2013/12/glosario-de-terminos-importantes-de.html

Cerini, D. & Prá, I. (2002). *Plan de Seguridad Informatica.* (Tesis de grado). Universidad Católica de Córdoba, Cordoba, Argentina. Available from: https://eduarmandov.files.wordpress.com/2017/05/security-plan-de-seguridad-informatica.pdf

Chanamé Orbe, R. (2015). *Hábeas Data y el Derecho Fundamental a la intimidad de lapersona*. (M. Eugenio Bustamante, Ed.). España. Available from: https://docplayer.es/6786568-Habeas-data-y-el-derecho-fundamental-a-la-intimidad-de-la-persona-chaname-orbe-raul-glosario.html

Echeverria, G. (2018). *Procedimientos y Medidas de Seguridad Informatica.* Perú. Available from: https://books.google.com.pe/books?id=64eIAgAAQBAJ&pg=PA212&lpg=PA212&dq=(Sistema+central)+computador+que+permite+a+los+usuarios+comunicarse+con+otros+sistemas+centrales+de+una+red.+Los+usuarios+se+comunican+utilizando+programas+de+aplicaci%C3%B3n,+tales+c

Eliasar. (2 de mayo de 2004). *Manual para identificar las partes de una PC e instalación de una grabadora de CD o DVD.* Available from: https://www.monografias.com/trabajos35/partes-computadora/partes-computadora.shtml

Ferrero Recasens, E. (2009). *Analisis y gestion de riesgos del servicio IMAT del sistema de informacion de I.C.A.I.* (Tesis de grado). Universidad Pontifica Comillas, Madrid, España. Available from:

https://es.scribd.com/document/243914039/Fases-de-Analisis-de-Riesgos-y-Gestion-MAGERIT

Galeon. (2018). Sistema Operativo MS-D.O.S. *Revista MS-D.O.S. 7.10.* Available from: http://tic154.galeon.com/productos1306524.html

Gobierno Digital. (2018). *Aspectos generales de la Seguridad de la Información*. *Libro 507 Metodologias*. Perú. Available from: http://www.gobiernodigital.gob.pe/publica/metodologias/Lib5007/21.htm

Gotzy. (mayo de 2017). *Elaboración de una metodología para implantar políticas de seguridad en los e-commerces.* (Tesis de E-commerce).

Hernández, R., Fernández, C., & Baptista, P. (2014). Metodología de la investigación (6a ed.). México.

Infante Ventura, R. (20 de agosto de 2018). *Seguridad en Sistemas y Computación.* Mexico.

Internet GLOSARIO. (23 de Junio de 2017). *internet, computadoras y algunas tecnologías de comunicación.* Available from: https://www.internetglosario.com/letra-h.html

Lamarca Lapuente, M. J. (29 de julio de 2018). *El nuevo concepto de documento en la cultura de la imagen.* (Tesis doctoral). Universidad Complutense de Madrid. Madrid, España. Available from: http://www.hipertexto.info/documentos/html.htm

Leyes. (2018). Ficheros .Bat o .Batch. *Diccionario Juridico.* Available from: https://www.drleyes.com/diccionario-juridico/ficheros-bat-o-batch

Marly. (17 de Julio de 2007). *Glosario.* Obtenido de Blogspot la vida tecnologica: http://lavidatecnologica.blogspot.com/

Matalobos Veiga, J. M. (2009). *Análisis de riesgos de seguridad de la información* (Tesis de grado). Universidad Politécnica de Madrid, Madrid, España. Available from: http://oa.upm.es/1646/

MATPEC. (2018). *Soluciones web*. Available from: http://www.matpec.com.ar/soporte/soporte-glosario-net.php#menu

Moncada Vigo, G. (2001). *Guía Practica para el Desarrollo de planes de cotingencia de sistemas de informacion.* Lima, Perú: INEI. Available from: http://www.academia.edu/8890033/Plan_De_contingencia_para_un_software

Pallas Mega, G. (2009). *Metodología de implantación de un SGSI en un grupo empresarial jerárquico.* (Tesis de maestría). Universidad de la República

Uruguay, Montevideo. Uruguay: Available from: https://www.colibri.udelar.edu.uy/jspui/bitstream/20.500.12008/2954/1/tesis-pallas.pdf

Pra, I. (mayo de 2016). *Plan de Seguridad Informatica.* (Tesis de grado). Universidad Catòlica de Còrdova, Cordoba, Argentina. Available from: http://docshare.tips/21156297-psi_574a5959b6d87f1a2d8b496e.html

Pressman, R. (1982). *Ingeniería del Software.* Mexico: McGraw Hill.

Rendón, A. (2018). Plan de Contingencia de los Sistemas de Información de 2018. Villavicencio, Colombia: Contraloria Municipalidad de Villavicencio. Available from: http://www.academia.edu/11282728/PLAN_DE_CONTINGENCIA_INFORMATICO

Román Medina, H.-H. (2002). *Análisis de seguridad, optimización y mejora de un portal web basado en PHP y MySQL*. (Proyecto). Escuela Superior de Ingenieros-Ingeniería de Telecomunicaión, Universidad de Sevilla, Sevilla, España. Available from: https://www.lawebdelprogramador.com/pdf/7051-Analisis-de-seguridad-optimizacion-y-mejora-de-un-portal-web-basado-en-PHP-y-MySQL.html

Root Secure. (11 de marzo de 2008). *Glosario de seguridad*. Root Secure :: The 2 faces of Security. Available from: https://rootsecure.wordpress.com/2008/03/11/glosario-de-seguridad/

Ruiz Calful, S. (28 de mayo de 2001). *Política oficial de SeguridadInformática del CICESE*. Available from: https://es.scribd.com/document/96825556/poli-segu

Sarmiento, A., & Callejas, U. (2000). Terminos. *Diccionario Econet.* Available from: http://www.angelfire.com/electronic/econetcol/diccionario5.htm

Segovia, C. (2001). Sistema integral de información para implementar un turismo para todos. Argentina. Available from: http://www.turismoaccesible.com.ar/seguridad/inf_virus.htm

SICE. (2018). *Comercio Electrónico.* Available from: http://www.sice.oas.org/e-comm/legislation/col2.asp

Sottile, C. E. (Mayo de 2016). *Sistemas Operativos.* Available from: https://www.monografias.com/trabajos38/historia-computacion/historia-computacion4.shtml

UCB. (2005). *Gestión de seguridad de la información*. (Universidad Católica Boliviana) Obtenido de Procdimientos de la Base de Datos: http://www.ucb.edu.bo/Procedimientos/BaseDeDatos/GestionDeSeguridadDeLaInformacion.htm

VICTDELR. (5 de marzo de 2013). *Guia para elaborar un plan de contingencia informatico.* Available from: https://victdelr.wordpress.com/

Villani Jiménez, D. A. (3 de Junio de 2018). Plan estratégico de las tecnologias de la información y las comunicaciones-PETI 2018-2020. *Revista Humanizate HFPS.* https://hfps.gov.co/wp-content/uploads/2018/07/PETI.pdf

ANEXOS

Anexo 1. Relevamiento inicial

Para el desarrollo de la presente auditoría fue necesario entrevistar a distintos usuarios del sistema y demás personas que interactúan con él. En el presente anexo se adjuntan los cuestionarios utilizados para la realización de éstas entrevistas.

1.1. Hardware

Topología y protocolos de red

- Protocolos.
- Conexión al exterior con sucursales y fábrica.

Características del servidor:

- Tipo o marca de servidor.
- Capacidad de procesamiento.
- Cantidad de memoria.
- Capacidad de disco.
- Placas de red.
- Dispositivos varios (CD's, cintas, scanner, switch, hub, etc.).
- UPS o sistemas de alimentación alternativa del servidor.
- Servidor alternativo, espejo de contingencia.
- Servidor de datos o de impresión.
- Impresoras y Gestión de impresión.

PC´s

- Cantidad.
- Características particulares.
- Terminales o PC´s.
- Clones o de marcas.
- Características generales.

Web

- Tipo de conexión.
- Permisos o acceso de las PC´s.
- Firewall y virus Wall.

- Página dinámica o estática.
- Servidor propio o web hosting..

Back up

- Disco espejo.
- Tercerización.
- Dispositivos de back up (CD's, cintas magnéticas, HD, disquete, etc.)

1.2. Software

Software del servidor

- OS.
- Aplicaciones.
- Motor de bases de datos.
- OS y software de las PC´s.
- Aplicaciones bases en cada sector de la empresa administración, ventas, cómputos, etc.

Gestión de virus

- Detalle de aplicaciones propias, enlatadas.
- Gestión de red física y lógica.
- Licencias.

1.3. Usuarios

Organigrama

Responsabilidades en área de informática

- Responsables de Redes.
- Responsables de Bases de datos.
- Responsables de Aplicaciones.
- Responsables de Servicio técnico.

Tipo de perfiles de usuarios según sectores

- Clasificación del perfil.
- Accesos del perfil a aplicaciones o datos.

Anexo 2. Seguridad lógica

2.1. Identificación – ID'S

2.1.1. Altas

- ¿Qué datos hay en el perfil del usuario cuando se hace un alta? ¿Se guardan los siguientes datos?

- ID de usuario,
- Nombre y apellido completo
- Puesto de trabajo y departamento de la empresa
- Jefe inmediato
- Descripción de tareas
- Consentimiento a que auditen sus actividades en el sistema, y de que conoce las normas de "buen uso" del sistema
- Explicaciones breves y claras de cómo elegir su password,
- Tipo de cuenta o grupo al que pertenece (empleado, gerente, etc.)
- Fecha de expiración de la cuenta
- Datos de los permisos de acceso y excepciones
- Restricciones horarias para el uso de recursos
- ¿Qué otros datos del usuario son necesarios en el ID? ¿Qué datos guardan en la planilla de personal?
- ¿El ID de usuario puede repetirse? ¿Y si una cuenta fue borrada o eliminada, puede utilizarse un ID ya usado y eliminado para un usuario nuevo?

2.1.2. Bajas

- ¿Cómo se relacionan con los de RRHH? ¿El departamento de RRHH se encarga de comunicar las modificaciones en el personal? ¿Qué se hace al respecto?
- ¿Cómo se actualiza la lista?
- ¿Cómo se administran los despidos (o desvinculación del personal)? ¿Se tiene en cuenta una política de despidos para evitar actos de vandalismo por posibles disgustos de los empleados desvinculados de la empresa?
- ¿Hay algún histórico de las cuentas que se dan de baja?
- ¿Se guardan los archivos y datos de las cuentas eliminadas? ¿Por cuánto tiempo?
- ¿Qué datos se guardan? ¿Con qué motivo?

2.1.3. Mantenimiento

- ¿Hay procedimientos para asignar los usuarios a un grupo de acuerdo a ciertas características? ¿Hay procedimientos para dar de alta, baja, modificar, suspender, etc. una cuenta de usuario?
- ¿Se hacen revisiones de las cuentas de usuarios? ¿Se revisan sus permisos?
- ¿Hay procedimientos para determinar los nuevos requerimientos relacionados con cambios en funciones del empleado? ¿Cómo se mantienen actualizadas las cuentas cuando esto pasa?
- ¿Se documentan las modificaciones que se hacen en las cuentas? ¿Se lleva un histórico de los cambios?

2.1.4. Permisos

- ¿Tienen una clasificación de los recursos (datos) en base a la sensibilidad? ¿O en base a los tipos ¿base de datos, archivos de configuración, datos personales, según el departamento de la organización?)? ¿Cómo se define la sensibilidad de los objetos?
- ¿Tienen distinción de los tipos de accesos que tiene cada usuario a cada recurso? (lectura, escritura, etc.)
- ¿Quién les asigna los permisos a los usuarios?

2.1.5. ID inactivas

- ¿Después de qué período de inactividad en que el usuario no realiza acciones en el sistema, se limpia la pantalla asociada al usuario, se desconecta el usuario inactivo o pide la password de nuevo?
- Antes de terminar con la sesión, ¿se avisa al usuario que se lo desconectará? Si en un determinado tiempo el usuario no responde, ¿entonces se termina la sesión?
- ¿Después de qué período de inactividad (de cuantos días) se pone una cuenta de usuario como inactiva, porque el usuario no se ha logeado? ¿Este proceso es automático (del sistema operativo) o lo realiza el administrador?

2.1.6. Acciones correlativas a usuarios

- ¿Los usuarios se identifican en forma única o existen usuarios genéricos que todas las personas usan? ¿Todos los usuarios tienen un perfil o pertenecen a algún grupo?
- ¿El sistema genera históricos o logs de las actividades de los usuarios en el sistema, para poder seguirles el rastro?

- ¿Tienen forma de asignar responsabilidades individualmente a cada usuario, identificándolo a través de su ID?

2.1.7. Grupos - Roles

- ¿Existen grupos de usuarios? ¿Cómo se forman los grupos? ¿Según el departamento de la empresa donde trabajen, según el rol que desempeñen? ¿Por qué esa clasificación?
- ¿El acceso puede controlarse con el tipo de trabajo o la función (rol) del que pide acceso?
- ¿Los ID hacen referencia a una persona, o son anónimos? ¿Hacen referencia a un grupo?
- ¿Se eliminan los que vienen por default en el sistema operativo? (Cuentas Guest, por ejemplo)

2.1.8. Súper usuario

- ¿Qué tipos de perfil de administrador hay?
- ¿Cuántas personas y quiénes son administradores?
- ¿Desde qué terminal puede logearse un administrador?
- Además de la cuenta de administrador, ¿tienen otra cuenta para las funciones comunes?

2.1.9. Display

- ¿Qué datos se muestran cuando alguien intenta logearse? ¿Se muestran los siguientes datos?
  - Nombre de usuario
  - Password
  - Grupo o entorno de red
  - Estación de trabajo
  - Fecha y hora
- ¿Qué datos se muestran cuando alguien logra logearse? ¿Se muestran los siguientes datos?
  - Fecha y hora de la última conexión.
  - Localización de la última conexión (Ej. número de terminal)
  - Intentos fallidos de conexión de ese ID de usuario desde la última
  - conexión lograda.

2.1.10. Varios

- ¿Utilizan el ID de usuario como un control de acceso a los recursos, o solo para ingreso al sistema?
- ¿Un usuario puede tener solo una sesión abierta, de alguna aplicación, de acuerdo a sus tareas o puede tener varias? ¿Depende de la cantidad de grupos a los que pertenezca?

2.2. Autenticación

2.2.1. Datos de autenticación

- ¿Cómo se protegen los datos de autenticación cuando están siendo ingresados por el usuario? ¿Qué se muestra en pantalla cuando se tipea el password?
- ¿Espacios, asteriscos, no se mueve el cursor?
- ¿Cómo se guardan los datos de autenticación en disco? ¿Encriptados? ¿Bajo password? ¿De qué forma se los asegura?
- ¿Cómo se restringe el acceso a estos datos? ¿Hay un control de acceso más severo con estos datos? ¿Se los clasifica como confidenciales?
- ¿Quién tiene acceso a estos datos?
- ¿Cómo se transfieren los datos de autenticación desde la terminal que se logea hasta el servidor encargado de autenticar? ¿Encriptados, o solo en texto plano?

2.2.2. Alcance de la autenticación

- ¿Qué alcances tienen las autenticaciones? ¿Es una autenticación para una aplicación en particular, para toda la red, o solo para la LAN, y otra para la WAN?

2.2.3. Límites de los intentos de logeo

- ¿Se lockea el usuario después de varios intentos fallidos de autenticación o se inhabilita la cuenta o la terminal?
- ¿Después de cuantos intentos?
- ¿Qué se hace después de la inhabilitación: se espera un tiempo y muestra nuevamente la pantalla de logeo o el administrador debe aprobar la operación de re-logeo?

2.2.4. Firmas digitales

- ¿Se usan firmas digitales para autenticar a los usuarios dentro de la organización, cuando mandan mensajes internos? ¿Y para mensajes externos?
- ¿Serían necesarias para algún documento?

- Interoperabilidad: ¿De qué forma se "ponen de acuerdo" Windows y LINUX para la autenticación? ¿Es necesaria esa interoperabilidad para algo? ¿Es necesaria alguna herramienta para esta comunicación?
- Separación de tareas: ¿Se manejan los controles de acceso de manera que una sola persona no tenga acceso a todo, en relación a una sola transacción?
- ¿Existe separación de tareas a través del control de acceso?
- Rotación de tareas: si existe rotación de tareas, ¿cómo es el mecanismo en el control de acceso para posibilitar esto? ¿Se modifican los permisos? ¿O tienen todos los permisos necesarios permanentemente?
- Vacaciones: ¿son obligatorias las vacaciones en la empresa? Si es así, ¿cómo se manejan con las passwords durante los períodos de vacaciones? ¿Qué ocurre con la cuenta del administrador en el período de vacaciones? ¿Puede ser modificada? ¿Cómo controlan que no sea modificada durante su ausencia?

2.3. Passwords

- ¿El password puede ser igual al ID del usuario?

2.3.1. Generación

- ¿Las passwords son generadas con procesos automáticos (programas de generación de passwords) o son creadas por los usuarios? ¿Se usan estos programas en alguna máquina, por ejemplo, en los servidores?
- ¿Qué características deben tener estas passwords?
- ¿Cuál es el conjunto de caracteres permitidos (alfa, numéricos y caracteres especiales)?
- ¿Cuál es el largo mínimo y máximo del password (seis a ocho, preferentemente nueve)?
- ¿La password se inicializa como expirada para obligar al cambio?
- ¿De qué forma se hace cumplir este requerimiento? ¿Se pone una fecha de expiración? ¿No se permite al usuario logearse ya que su password ha expirado?
- ¿Se chequean contra un diccionario online para verificar que no sean palabras que existan?
- ¿Se permite que contengan el nombre de la empresa, o el nombre del usuario?
- ¿Dos cuentas pueden tener las mismas passwords?
- Si existe más de una cuenta de administrador, ¿algunas de estas (o todas) tienen las mismas passwords?

2.3.2. Cambios

- ¿Qué procedimiento existe para el cambio de las passwords de los usuarios?
- ¿Se puede cambiar en cualquier momento? ¿Quién puede hacer los cambios?
- ¿El administrador? ¿Los usuarios a través de una opción en el menú? ¿Le tienen que avisar a alguien cuando cambian la contraseña? ¿Tiene que pedir autorización? ¿Qué procedimiento existe para comprobar que las passwords asignadas por default (por el administrador o por el sistema operativo) han sido cambiadas por el usuario?
- ¿Cuál es el procedimiento para manejo de password pérdidas o reveladas? ¿Cómo se cambian? ¿Solo se cambia la password o se cambia también la cuenta y el nombre del usuario?
- ¿Con qué frecuencia es necesario cambiar la password antes que se vuelva obsoleta? Al modificar la password de una cuenta, ¿se puede repetir la misma password? ¿Se guarda una base de datos con las últimas password de los usuarios? ¿Cuántas passwords de cada usuario se guardan?

2.3.3. Entrenamiento a usuarios

- ¿Se entrena a los usuarios en la administración del password? ¿Se les enseña a no usar passwords fáciles de descifrar? ¿no divulgarlas? no guardarlas en lugares donde se puedan encontrar? entender que la administración de passwords es el principal método de seguridad del sistema?

2.4. Control de acceso lógico

- **Modelos de control de acceso:** ¿Siguen algún tipo de modelo o mecanismo estándar de control de acceso? ¿Sería factible y económico implementar uno?
- **Aplicación:** ¿para el control de acceso usan una aplicación? ¿Cómo se administra? ¿Qué características tiene? ¿Esta aplicación es: ¿Propia del sistema operativo? ¿De aplicación y programas propios o comprados? ¿Con paquetes de seguridad agregados al sistema operativo?

2.4.1. Criterios de acceso

- ¿Qué criterio usan para el control de acceso? ¿Alguno de los siguientes?: Identidad (ID de usuario) Roles
- **Localización:** ¿existen controles de acuerdo a la localización de la información?
- **Recursos:** ¿se pide un password cada vez que alguien quiera entrar a una carpeta compartida del servidor de Linux? ¿El password que los usuarios ingresan para la

aplicación de la empresa sirve para explorar el sistema y así poder ver las carpetas de los servidores? ¿Es necesario poner otro password además del login?

- **Tiempo:** ¿se limita el momento del día (o del año) en el que un usuario puede entrar al sistema? ¿Cómo? ¿Qué días, horas? ¿Con qué aplicación? Limitaciones a los servicios: ¿Existen restricciones de servicio? ¿Cómo?
- **Modos de acceso:** ¿Si el acceso es desde módem existen distintos permisos que desde terminal? ¿Se toma en cuenta el número de teléfono al comunicarse vía módem? ¿Usan un sistema call-back?
- **Transacción:** ¿se permite hacer ciertas transacciones a unos usuarios que otros no pueden hacer? ¿Dependiendo de qué? ¿Del tipo de usuario y del grupo? Aplicación: ¿se restringe el acceso a ciertos programas a ciertos usuarios? ¿Cómo?

2.4.2. Mecanismos de control de acceso interno

- ¿Cuáles de estos mecanismos de control de acceso se usan?
- Passwords, Listas de control de acceso (ACL)
- ¿Existe una ACL o matriz, o algo similar donde se especifiquen los usuarios y los accesos que tienen?
- ¿Qué sería más conveniente, una lista o una matriz? ¿Por qué?
- ¿Con qué aplicaciones se manejan? ¿Con alguna del sistema operativo, o con otro software?
- ¿Cómo se actualiza? ¿En forma manual o, si se modifica la lista de usuarios del sistema, se actualiza automáticamente la ACL? ¿Con qué frecuencia se revisa y actualiza?
- ¿Se usa encriptación para almacenarla? ¿Se protege de alguna manera? ¿Qué sería lo mejor y por qué para protegerla?
- Interfaces de usuarios restringidas
- ¿Se restringen las interfaces que ven los usuarios, (como el escritorio de Windows) de manera que los usuarios solo vean lo que les está permitido?
- ¿Cómo se hacen las restricciones? ¿Con la vista de menús?
- ¿Los usuarios solo ven una determinada vista o ciertas tablas de las bases de datos?
- Encriptación: ¿se encriptan algunos datos? ¿Cuales?
- ¿Las ACL?

- ¿Los mensajes?
- ¿Las passwords y datos de las cuentas de usuarios?
- ¿Los datos de configuración?
- ¿Los datos críticos de la empresa?
- ¿Los datos que están siendo transmitidos (internamente en la LAN o externamente a través de Internet o el módem)?
- Protección de puertos: ¿usan dispositivos externos físicos para proteger el puerto de los intrusos (llaves de hardware, por ejemplo)?

2.4.3. Control de acceso externo

Mecanismos de control de acceso externo:

- ✓ Gateway (puertas de seguridad) o firewalls seguros
- ✓ Acceso de personal contratado, consultores o mantenimiento.
- ✓ Autenticación basada en host: ¿existe una autenticación que da acceso al sistema basándose en la identidad del host que pide el acceso, y no en la identidad del usuario que quiere entrar?
- ✓ ¿Existe acceso externo a los datos, desde Internet o desde el módem? ¿Quién tiene ese acceso?
- ✓ ¿Qué procedimientos se tienen en cuenta para mantener la integridad y la confiabilidad de los datos? ¿Se tienen en cuenta los siguientes?
- ✓ ¿Alguna forma de identificación o autenticación?
- ✓ ¿Control de acceso para limitar lo que se lee, ve, borra, modifica, etc.?
- ✓ ¿Firmas digitales?
- ✓ ¿Ponen las copias de seguridad de la información pública, en otro lado, no en la misma máquina?
- ✓ ¿Prohíben el acceso público a bases de datos “vivas” (live data base o bases de datos)?
- ✓ ¿Verifican que los programas y la información pública no tenga virus?
- ✓ ¿Passwords one-time?
- ✓ ¿Están separados los datos que se publican en Internet de los datos del interior de la empresa?
- ✓ ¿Son los mismos datos o están en PC’s diferentes?

- ✓ ¿Usan alguna forma de acceso remoto para cambiar las configuraciones de un sistema?

2.5. Sistema de Detección de Intrusos (IDS)

- ¿Ha habido intentos de intrusión? ¿Vale la pena implementar un sistema como estos?
- ¿Se usa algún software de IDS? ¿Son tolerantes al fallo? ¿Usan muchos recursos? (Ejemplos: OmniGuard, RealSecure, Cisco Secure IDS)
- ¿Se usan herramientas de monitorización de red para encontrar intrusos?
- ¿Se releen los logs de auditoria buscando pistas de IDS? ¿Se buscan algunas de las siguientes?
- Muchos intentos fallidos de autenticación.
- Tráfico excesivo de red.
- Muchas violaciones a permisos.
- Si hubiera una entrada de un intruso, ¿se documenta? ¿Qué medidas se tomarían (o tomaron) para que no ocurra más?

2.6. Denial of Service

- ¿Se llevan a cabo algunas de las siguientes actividades?
- ¿Instalan ACL en los routers?
- ¿Quitan los servicios de red no necesarios o no utilizados, por ejemplo: ECHO, etc.?
- ¿Separan los datos críticos de los que no lo son, a través de lo que haya disponible, como, por ejemplo: sistemas de cuotas (disk QUOTAS, o particiones,? ¿o volúmenes)?
- ¿Establecen valores base para la actividad normal, en cuanto a memoria, utilización de disco, de la CPU o tráfico de red?
- ¿Usan herramientas para detectar cambios en la configuración o en los archivos?
- ¿Usan configuraciones redundantes de red y tolerantes a fallos?

Anexo 3. Seguridad en las comunicaciones

3.1. Configuración de red

3.1.1. Activos de la red

- ¿Cómo es la topología de la red? ¿Existe un inventario o gráfico topológico? Debería incluir lo

  Siguiente:

  - switch,
  - routers,
  - hub's,
  - modem,
  - PC's,
  - conexiones de radio,
  - fibra óptica, etc.
- ¿Cuantos dispositivos de esta lista hay y en qué forma están ubicados y utilizados?
- ¿Qué filtros tiene cada uno de estos dispositivos?
- ¿Existe encriptación a nivel de hardware?
- ¿Por qué pusieron un switch en lugar de un router? ¿Por el costo? ¿Por el tamaño de la red? ¿Por qué implementaron un sistema radial? ¿Es demasiado inseguro? ¿No es muy caro?

3.1.2. Servidor de Hosting

- ¿Qué se tuvo en cuenta para elegir ese servidor de hosting?
  - Precio,
  - Medidas de seguridad,
  - Respaldo en caso de emergencia, de caída del servidor y de pérdida de info.
- ¿Qué características tienen los servidores? (de mail, de Internet, de datos o aplicaciones). ¿Causa alguna dificultad que el servidor esté físicamente lejos de las sucursales?

3.1.3. Comunicaciones

- ✓ Con respecto al MODEM con el que se comunican con la fábrica:
- ✓ ¿Pasa por el firewall?
- ✓ ¿Los datos van encriptados?

- ✓ ¿Se realizan los controles de acceso adecuados a los servidores que se encuentran conectados a Internet?

3.1.4. Recursos compartidos

- ¿Se comparten los discos de las PC's en la red? ¿Por qué?
- ¿Qué carpetas comparten?
- ¿Se pueden ver las carpetas de los mails de mis compañeros?
- ¿Tienen contraseñas estas carpetas? ¿Quién pone las contraseñas: el dueño de la información o el administrador?

3.1.5. Configuración de puertos

- ¿Se deshabilitaron los puertos que no son necesarios? ¿Cuáles? ¿De qué protocolos o servicios? ¿Quién lo hizo?
- ¿Se prueban los puertos de la red? ¿Y el firewall? ¿Con qué herramientas?
- ¿Se ha hecho una prueba de auto hackeo?
- ¿Con qué herramientas se prueban o pueden probar los puertos? ¿Solo con el SQuid? ¿Por qué no usaron otro programa?

3.1.6. Testeo mensual de la red

- ¿Se hace algún chequeo periódico de la red y sus permisos?
- ¿Qué se controla?
- ¿Se documentan la ejecución y los resultados de estas pruebas?

3.1.7. Acceso remoto

- ¿Cómo se mantienen las máquinas con Linux? ¿Vía acceso remoto? ¿Quién las mantiene
- ¿Qué herramientas se usan? ¿Cómo funciona la herramienta?
- ¿Se debe cambiar la configuración del firewall para hacer este acceso remoto?
- ¿Qué servicios son necesarios para el mantenimiento (HTML, FTP, IP, DNS, TELNET)? ¿El firewall no tiene restricción en ese servicio, se le saca la restricción del servicio al firewall o solo habilito una dirección específica, la de la máquina desde donde se hace el mantenimiento?
- ¿Qué es lo que se mantiene con este sistema?
- ¿Cómo se aseguran que no entren llamadas, sino que solo salgan los pedidos?

3.1.8. Medidas de fiabilidad

- ¿Existen medios alternativos de transmisión de datos en caso de que exista alguna contingencia con la red? ¿Que se haría si se cae un nodo? ¿Está prevista esa situación?
- ¿Existe una redundancia de acceso a Internet? (si no funciona ADSL tener un dial up configurado).

3.2. Mail – Chat

3.2.1. Herramientas

- ¿Con qué herramienta administran el correo en el servidor y cómo se hace?
- ¿Es una herramienta del sistema operativo? ¿Es comprada? ¿Por qué eligieron esa?
- ¿Es configurable?
- ¿Quién es el encargado de su configuración?
- ¿Se chequea periódicamente que la configuración sea eficiente? ¿Con qué frecuencia? ¿Se encuentran errores?
- ¿Se actualiza a las versiones más nuevas de esta herramienta? ¿Cómo se enteran de las nuevas versiones?
- ¿El servidor de mail es el mismo que el servidor de Internet o el de aplicaciones?
- ¿Con qué herramienta los usuarios leen su mail? ¿Lo hacen desde sus PC's?
- ¿Qué configuraciones tienen estas herramientas?
  - ✓ Habilitada la vista previa
  - ✓ Confirmación de lectura
  - ✓ Block sender
  - ✓ Chequeo de virus en correo entrante y saliente
  - ✓ Controles ACtiveX y Scripts
- ¿Quién las configura? ¿Los usuarios o el administrador? ¿Todas las PC's tienen la misma configuración?
- ¿Cómo configuran el IncrediMail?
- ¿Se le deshabilitan las mismas características que nombré arriba?

3.2.2. Proceso de recepción y envío de mails

- ¿Cómo es el proceso de recepción de mail? ¿El servidor baja los mails de toda la empresa a sus discos, y luego los reparte a sus destinos?
- ¿Los mails se borran del servidor cuando son descargados a la máquina del usuario? ¿O no se borran nunca del servidor? ¿Cómo es esta política?

- ¿Los mensajes están comprimidos dentro del servidor?
- ¿Automáticamente se envían los mails a cada cuenta de usuario cuando llegan al servidor o se guardan en disco del servidor y se envían en un determinado momento (por ejemplo, varias veces al día, o cuando el usuario lo solicita)?
- Al recibir cualquier tipo de mail, ¿existen mecanismos de filtrado que nos permiten buscan ciertas frases o palabras dentro del encabezado o cuerpo del mensaje? ¿Podemos determinar si hay algún mail con un determinado asunto, de manera de evitar los virus o los correos no deseados?

3.2.3. Espacio en disco

- ¿Cómo se administra la capacidad de disco asignada a los mails?
- ¿Se asigna un espacio de disco a la totalidad del correo?
- ¿Se asigna un espacio de disco a cada usuario del mail?
- ¿Se asigna un espacio de disco a cada cuenta de mail?
- ¿Se asigna un espacio de disco a cada departamento?
- ¿Existen distintas cantidades asignadas a los usuarios de acuerdo a su perfil o grupo, o todos los usuarios tienen la misma cantidad de espacio en disco?
- ¿Qué pasa si se llega al límite de espacio en disco asignado? ¿Ha pasado alguna vez? ¿Se le avisa al usuario correspondiente que limite el uso de su cuenta de mail? ¿Se puede suspender solo su servicio de mail sin afectar el resto de la empresa?
- ¿Cuándo se suspende la recepción de mails? ¿Cuándo se ha llenado el servidor o antes, para poder hacer algo para vaciarlo?
- ¿Existe un límite para los mensajes de salida o de entrada?

3.2.4. Mail Interno y Externo

- ¿Existen direcciones de mail para todos los empleados? ¿Solo algunos empleados tienen? ¿De qué depende este servicio?
- ¿Ese mail es interno o también existe una casilla para mail externo para cada empleado?
- ¿Cómo funciona el mail interno, va al hosting y después al servidor de correo o va directamente al servidor de correo?
- ¿Existe algún tipo de control para asegurarse que los usuarios no usan el mail de la empresa para fines personales sino para su trabajo?

- ¿Se controla que no se suscriban a listas de correo o cadenas de mails con esta dirección de mail?
- ¿Controlan los SPAMS en estas direcciones? ¿Cómo lo hacen?
- Al enviar mails hacia todos los empleados, ¿la lista se oculta con el CCO o copia oculta, o se los lista en el campo de TO?
- ¿Permiten el conocimiento público de las direcciones externas de mails de los empleados?
- ¿Están publicadas en Internet o solo las administran sus propietarios?
- ¿Existen direcciones de mails destinadas a la comunicación con el cliente, como el libro de quejas, consultas, etc. (Ej. ventas@laempresa.com)? ¿En dónde se encuentran? ¿Quién las administra? ¿El departamento correspondiente o el administrador de web?

3.2.5. Correo basura

- ¿Cómo se identifica al correo basura?
- ¿Cómo se administra el correo basura?
- ¿Con qué herramienta lo hacen? ¿Cómo se configura?
- ¿Cómo se define qué es correo basura y qué no?
- ¿Qué pasa si a una cuenta llega gran cantidad de correo basura?
- ¿El correo basura se elimina directamente o es posible generar logs para su posterior análisis?
- ¿Qué conclusión se ha sacado de esos análisis?
- ¿El correo basura se baja hasta el servidor de mails y desde ahí se elimina, o directamente se elimina antes de ser bajado, en el ISP? ¿Cómo lo administra el ISP?

3.2.6. Chat

- ¿Se permiten los servicios de chat?
- ¿Cuáles se usan? MSN, ICQ, Yahoo! ¿Chat? ¿Otros?
- ¿Se permite bajar archivos a través de estos programas?
- ¿Se usan programas de file sharing (Morfeus, Kazaa, Napster, Audio Galaxy, iMesh, eDonkye2000? ¿etc.)?

3.2.7. Copia de seguridad

- ¿Se genera una copia de seguridad de los mensajes enviados y recibidos? ¿De todos? ¿Se guardan en el disco? ¿Se comprimen?

- ¿Se hacen back up de las carpetas del SendMail (como las dbx del Outlook
- Express)?
- ¿Se imprimen para su control o para que conste en algún archivo en papel?
- ¿Poseen un sistema propio de mail record definido o alguna herramienta automática de gestión de mails record?

3.2.8. Privacidad – Firma digital – Encriptación de mails

- ¿Prohíben el envío de archivos de la empresa u otros documentos confidenciales vía mail?
- ¿Se toman medidas de seguridad especiales cuando el mensaje de salida tiene datos confidenciales? ¿Se exige que vaya firmado, o encriptado? ¿Se exige que la dirección de destino sea conocida o confiable?
- ¿Se utiliza la firma digital en algún tipo de mensajes? ¿Qué tipo de firma se usa?
- ¿Se usa para mensajes externos e internos?
- ¿La clave privada de la firma digital es realmente privada, o la utilizan las secretarias (por ejemplo) para mandar mensajes en nombre de sus jefes? ¿Cómo se controla esto?
- ¿Utilizan la priorización de mail para la encriptación de los mismos?
- ¿Que sería importante proteger, en el caso de mensajes internos y externos?:
- ¿Integridad?
- ¿Confidencialidad?
- ¿No repudio?
- ¿Autenticación del remitente?
- ¿Se pide generalmente una confirmación de lectura en los mails salientes? ¿En todos, solo en los que tienen datos confidenciales, o cuando el usuario los configura?
- ¿Se encriptan los datos confidenciales que se guardan en disco (ejemplo: EFS – Encrypted File System - de Microsoft)?
  - ¿Archivo con contraseñas?
  - ¿Archivos de configuración?
  - ¿Archivos top secret?
  - ¿Qué otros datos se encriptan?

3.3. Virus – Antivirus

3.3.1. Herramientas

- ¿Cuáles de éstas medidas o herramientas poseen para evitar los virus?
- Paquetes de software antivirus
- Firewalls
- Sistemas de detección de intrusos
- Monitorización para evaluar el tráfico de red y detectar anomalías, como la acción de troyanos.
- Creación de un disco de rescate o de emergencia
- Procedimientos para cuando ocurra una infección con virus.
- Hardware de seguridad de red dedicado
- Back up de datos
- ¿Está habilitada alguna herramienta antivirus mientras se envían y reciben mails? ¿Cuál? ¿Por qué se usa esa?
- ¿Están seguros que detecta los virus y los elimina correctamente?
- ¿Han probado con otra herramienta?
- ¿Qué precio tiene el antivirus que compran? ¿Y las actualizaciones?
- ¿Hay un antivirus instalado en cada PC (incluyendo los servidores) o hay un solo antivirus en toda la red?
- ¿Qué significa que el antivirus sea corporativo? ¿Uno para los servidores y otra versión para los clientes? ¿En qué se diferencian?

3.3.2. Mensajes infectados – Procedimientos

- ¿Se han detectado mensajes infectados? ¿Qué problemas trajo? ¿Era de Windows o de Linux? ¿Cómo lo solucionaron?
- Si se encuentra un mail con virus, ¿qué se hace para que no lleguen más de esa misma persona? ¿Se identifica la fuente del mail, para bloquearla desde el router o desde el servidor de correo? ¿Se avisa al ISP para que no deje entrar más mails de esa dirección? ¿Se observan los headers de los mails para identificar su origen verdadero?
- Si las disqueteras están activadas en las PC's de los usuarios, ¿cómo se aseguran que los usuarios analicen los disquetes antes de abrir archivos?
- ¿Se generan disco de rescate con el antivirus? ¿Para todas las máquinas o solo para los servidores? ¿Quién es el encargado de esto? ¿Alguna vez han sido necesarios?
- ¿Cómo es la protección contra el mail-bombing? ¿Qué medidas se toman?

- ¿Suspenden la recepción de mail cuando el servidor está ocupado en un determinado porcentaje de su capacidad (80% por ejemplo)?
- ¿Qué procedimiento siguen en el caso de una infección con un virus?
- ¿Cada cuánto se hace un escaneo total de virus en los servidores? ¿Quién se encarga? ¿Se hace automáticamente cada vez que hay una actualización o periódicamente?
- ¿El escaneo de las maquinas se realiza por cuenta de cada usuario o lo realiza el encargado de sistemas? ¿No sería más seguro que el encargado lo haga a intervalos regulares de tiempo?
- ¿Qué prioridad tiene el SendMail?
- ¿El firewall tiene algo que ver con el análisis de los virus, o solo se encarga de los servicios de la red? ¿El antivirus y el firewall están relacionados de alguna forma, son compatibles entre sí? Ej. Firewall y antivirus de Norton se complementan para generar un nivel de seguridad superior.
- ¿Cómo se realiza el download de los mails desde el servidor hasta las PC's? ¿Cada PC se identifica según el usuario que se logea? ¿O es según el número de terminal de la PC en la red? ¿Se puede configurar una cuenta (Ej.: la de algún Gerente) en otra máquina (que no sea la del Gerente) y bajar los mails desde ahí?

3.3.3. Actualización de antivirus

- ¿Cómo se actualizan las definiciones de virus? ¿Quién las baja de Internet?
- ¿Quién ejecuta las actualizaciones en la PC's? ¿Cómo se enteran de las nuevas actualizaciones de virus?
- ¿Cuánto tiempo lleva diseminar y actualizar el antivirus en toda la organización?
- ¿Se hacen chequeos ocasionales para ver si se han actualizado los antivirus?

3.4. Documentación - Normas

- ¿Qué documentación existe de la red?
- ¿Diagramas topológicos?
- ¿Procedimientos?
- ¿Manuales?
- ¿Certificados (Ej.: de calidad, etc.)?
- ¿Licencias de software?
- ¿Planes de contingencia, de seguridad, etc.?

- ¿Contratos (Ej.: responsabilidades y mecanismos de transmisión al establecer una comunicación con las fábricas)
- ¿Cambios realizados en la configuración de la red?
- ¿Qué más? ¿Poseen cada uno de estos elementos de documentación de la empresa?:
- Manual de uso del software y de hardware usado (del software desarrollado y del comprado).
- Diagramas de red y documentación de la configuración de routers, switches y dispositivos de red.
- Procedimientos de emergencia (plan de contingencia)
- Plan de seguridad
- Manual de procesos estándares del Sistema Operativo (en especial de Linux)
- Métodos para compartir datos entre sistemas (por ejemplo, con las fábricas, entre las sucursales o entre las PC´s de la red)
- ¿Se han instalado correctamente todos los parches de seguridad disponibles del sistema operativo y de los programas usados? ¿Cómo se conoce de los parches? ¿Están suscriptos a un mailing list?
- ¿Hay alguna documentación donde se anote la configuración de las PC´s en la red? ¿Sus números IP, sus placas de red, etc.?

3.5. Ataques de red

- ¿Han tenido algún ataque en la red? ¿Que se ha hecho para arreglarlo? De los siguientes métodos contra los ataques más comunes, ¿qué está implementado?

Denial of service:

- ¿Hay herramientas Anti DoS?
- ¿Limitan el tráfico de red?
- ¿Generan una “baseline” o líneas de base con la actividad normal del sistema?
- ¿Se hizo alguna simulación ocupando una gran cantidad de recursos de algún tipo?
- ¿Instalan los parches de seguridad del sistema operativo?
- ¿Implementan un sistema de cuotas (Disk Quotas)?
- ¿Utilizan alguna herramienta para detectar cambios en la información de configuración u otros archivos (como Tripwire)?

Sniffing:

- ¿Las líneas de comunicación se segmentan tanto como sea práctico?
- ¿Los datos de logeo y otros datos sensibles son transmitidos encriptados?
- ¿Las cuentas privilegiadas (como root) se logean usando passwords one time o shadow passwords, y autenticación fuerte?

Spoofing:

- ¿Tienen alguna herramienta anti-spoofing?
- ¿Los routers son configurados para que rechacen los ataques de spoofing?
- ¿Solo los hosts apropiados son definidos como confiables en el Linux (como el /etc/hosts.equiv)? ¿Y este archivo tiene los permisos restringidos?
- Por más que el acceso externo esté prohibido, ¿se configura el control de acceso para denegar cualquier tráfico de la red externa que tiene una dirección fuente que debería estar en el interior de la red interna?

Ataque a las passwords:

- ¿Dónde se guardan las password del sistema operativo? ¿En el archivo /etc/passwd y /etc/group?
- ¿Se chequean regularmente las passwords para comprobar su consistencia los archivos que nombré arriba?

3.6. Firewall

- ¿Qué firewall usan?
- ¿En qué máquina (servidor) se encuentra el Firewall? ¿En una máquina dedicada? ¿En el servidor de Internet?

3.6.1. Tipos de firewall

- ¿Qué tipo de firewall hay?
- ¿Gateway de filtrado de paquetes (Packet Filtering Gateways)?
- ¿Gateway de aplicación?
- ¿Gateways híbridos o complejos?
- ¿Otro?

3.6.2. Política de configuración

- ¿En base a qué criterios definieron las configuraciones del firewall?

- ¿Tienen una política definida en cuanto a la configuración del firewall?
- ¿Usan una política de acceso a servicios?
- ¿Usan una política de dial-in y dial-out?
- ¿Usan una política de diseño y configuración del firewall? ¿Alguna de estas dos?:
- Postura de negación preestablecida: se especifica sólo lo que está permitido y se prohíbe todo lo demás:
- ¿Se examinan los servicios que los usuarios necesitan?
- ¿Se considera como afectarían la seguridad tales servicios y como se los puede proporcionar a los usuarios de manera segura?
- ¿Se permiten sólo los servicios que se comprenden o se tiene experiencia, que se pueden proporcionar con seguridad y para los cuales existe una necesidad legitima?
- Postura de permiso preestablecido: se especifica sólo lo que está prohibido y se permite todo lo demás.

3.6.3. Características del firewall

- ¿Qué controles de acceso tiene el firewall? ¿Qué servicios tiene habilitados y cuáles deshabilitados?
- ¿Soporta autenticación? ¿Con qué técnica? ¿Incluye las direcciones NAT (Network address translation) en la autenticación? ¿Y passwords?
  - ✓ ¿Qué habilidades tiene para monitorizar la red? Incluye:
  - ✓ ¿Intentos no autorizados de ingreso?
  - ✓ ¿Genera logs?
  - ✓ ¿Provee reportes? ¿O mails?
  - ✓ ¿Tiene alarmas?
- ¿Es lo suficientemente rápido para que no demore a los usuarios en sus intentos por acceder a la red (cómo es su performance)?
- ¿Qué tan configurables son sus opciones?
- ¿Puede adaptarse a distintas configuraciones de red o de sistemas (es escalable)?
- ¿Es fácil de configurar?
- ¿Es fácil de usar?
- ¿Es fácil de mantener?
- ¿Tiene un buen servicio postventa?
- Si se cae el firewall, ¿qué pasa? ¿Es una “falla segura”?

- ¿Se hizo alguna prueba de la configuración del firewall? ¿Trató de hacerse un intento de entrada sin autorización, por ejemplo?

3.7. Configuración de servicios y protocolos de red

De todos estos servicios:

- ¿Cuáles se usan en la red?
- ¿Cómo están configurados?
- ¿Están habilitados o prohibidos?
- ¿Existen excepciones?
- ¿Poseen acceso de entrada y/o salida?
- ¿Qué pasa con los otros puertos que quedan libres?
- ¿Se desactivan completamente los siguientes servicios o protocolos?

SUID (set user ID), RLOGIN, RSH, REXEC (Comandos "r" Remote), SU (SuperUser), NetStar, GOPHER, TFTP (Trivial File Transfer Protocol), Telnet, SYSTAT, FINGER, TALK, EXPN, VFRY.

- ¿Cómo se configuran los siguientes servicios o protocolos?
- POP (Post Office Protocol), MIME, HTTP, SMTP, FTP, Applets, Pruebas Cgi, Scripts Query, SHELL, NIS.

3.8. Herramientas para administración de red y protocolos

- ¿Usan alguna de estas herramientas o protocolos para la seguridad de la red?
- Tcp-wrappers, Netlogv, Satan, AntiSniff, Cops, SafeSuite, Gabriel,
- Courtney, Tcplist, SSL (secure socket layer), SHTTP, SMIME, NOCOL (Network Operations Center On-Line).
- ¿Las herramientas que se usan tienen las siguientes funciones?
- ¿Pueden monitorear y filtrar peticiones entrantes a distintos servicios?
- ¿Cómo lo hacen? ¿Con qué aplicación?
- ¿Indican la hora, la máquina origen (el número de IP) y el puerto de esa conexión?
- ¿Pueden seguir una traza de todos los intentos de conexión tanto admitidos como rechazados?
- ¿Se monitorea la red buscando ciertos protocolos con actividad inusual?

Se controlan los siguientes:

- Conexiones tftp,
- Accesos vía rsh (remote shell),
- Comandos en el puerto de sendmail como vrfy, expn, etc.
- Algunos comandos de rpc (remote procedure call) como el rpcinfo,
- Peticiones al servidor de NIS,
- Peticiones al demonio de mountd.

- ¿Se llevan estadísticas de uso de los protocolos?
- ¿Se puede utilizar para detectar cambios en los patrones de uso de la red, y todo aquello que nos puedan hacer sospechar que algo raro está pasando en la misma?
- ¿Se audita el tráfico IP?
- En la captura de paquetes IP, ¿se le puede especificar condiciones de filtrado como protocolos específicos, nombres de máquinas, etc.?
- ¿Tienen la posibilidad de filtrar paquetes Por hardware o por software?
- ¿Van creando una base de datos de todas las máquinas chequeadas y las va relacionando entre ellas (Satan es una herramienta que hace esto)?
- ¿Qué otra funcionalidad no nombramos que si tiene la herramienta usada?
- ¿Qué función sería muy útil al trabajar en la red?
- ¿Se mantiene actualizado el software? ¿Se investiga para mantener actualizadas las herramientas? ¿Alguien está a cargo de esta actividad?
- ¿Se buscan herramientas nuevas que faciliten la tarea? ¿Consultan a algún Organismo (como el CERT)?

Anexo 4. Seguridad de las aplicaciones

4.1. Elección del sistema a usar

- ¿Se hicieron los siguientes cuestionarios al elegir los sistemas operativos y programas usados en la empresa? ¿Qué respuestas tenían?
- Para todo tipo de sistemas se debe tener en cuenta los siguientes requisitos:
- Requerimientos funcionales: ¿qué funciones debe cumplir el sistema?
- Entorno necesario: ¿Windows, Unix o Linux?
- Requerimientos de compatibilidad: ¿se ajusta a estándares o a regulaciones internacionales, o a programas existentes en la empresa?
- Requerimientos de performance: respuestas por segundo, errores, etc.
- Requerimientos de Inter operatividad: ¿cómo se relaciona con los demás sistemas?
  - Fiabilidad: errores tolerables del sistema
  - Amigable: fácil de usar.
  - Precio y precio adicional de mantenimiento
  - Documentación y manuales propios del software
  - Además, hay que tener en cuenta los siguientes requisitos de seguridad Identificación y autenticación, Control de acceso, Login, Evaluación de protocolos, Incorruptibilidad, Fiabilidad,
  - Seguridad en la transmisión, Back up de datos, Encriptación, Funciones para preservar la integridad de datos, Requerimientos sobre privacidad de datos.

4.2. Control de datos de aplicaciones

- ¿Existe un control de cambios para los archivos del sistema o para las bases de datos de la empresa, como por ejemplo una base de datos, que se modifique cada vez que alguien haga una modificación sobre un archivo?
- ¿Existen restricciones de datos de salida, por ejemplo, al portapapeles o a la impresora, y otros?
- ¿Cómo es el acceso a las librerías de programa (o a la carpeta “Archivos de programa”)?
- ¿Cómo se asegura la confidencialidad de los datos en una laptop? ¿Qué datos hay en las laptops de la empresa, o de los usuarios?
- ¿Se generan logs en cada transacción de manera de poder hacer un “undo”?
- ¿Estos registran los cambios en los datos críticos del sistema?

- ¿Se generan históricos de auditoria indicando qué procesos se corrigieron, quién los corrigió y qué cambios hizo (control de cambios – gestión de configuración)? ¿Los archivos de programa y los de trabajo se almacenen en directorios separados?

4.3. Control de datos en el desarrollo

- ¿Se asegura la integridad, exactitud y validez de los datos de entrada y salida de las aplicaciones?
- ¿Las variables, parámetros y / o fórmulas de cálculo se incluyen en tablas o archivos separados de los programas, para facilitar su modificación?
- ¿Existe un proceso de control de cambios para el desarrollo? ¿Cómo se documentan estos cambios?
- ¿Controlan el contenido de los archivos de entrada? ¿Controlan que existan los archivos antes de ejecutar el programa?
- ¿Se hacen controles sobre la validez de los datos ingresados manualmente? (Controles de integridad de datos)
- ¿Se controla la consistencia de los datos de salida de las aplicaciones?
- ¿Las aplicaciones se operan a través de menús obligatorios o es a través de comandos del sistema? ¿Los operadores de estas aplicaciones pueden editar los datos reales del mismo (o sea las bases de datos)?

4.4. Seguridad de bases de datos

- ¿Los archivos de la base de datos tienen control de acceso? ¿O solo se hacen controles en las aplicaciones?
- ¿Se controlan las siguientes ocurrencias?
  - Tiempo y duración de los usuarios en el sistema
  - Número de conexiones a bases de datos
  - Número de intentos fallidos de conexiones a bases de datos
  - Ocurrencias de deadlock con la base de datos
  - Estadísticas de entrada-salida para cada usuario
  - Generación de nuevos objetos de bases de datos
  - Modificación de datos
- ¿Se hace algún chequeo regular de la seguridad de la base de datos? ¿Se documentan los chequeos incluyendo lo siguiente?
- ¿Se hacen y son efectivos los backups y los mecanismos de seguridad?

- ¿Hay algún usuario de la base de datos que no tenga asignado un password?
- ¿Hay algún usuario que no ha usado la base de datos por un período largo de tiempo?
- Además del administrador de datos, ¿quién tiene acceso a los archivos del software de base de datos, a los del sistema operativo y a las tablas del sistema (FAT)?
- ¿Quién puede ejecutar un editor SQL?
- ¿Quién tiene acceso de lectura – escritura a los archivos de programa?
- ¿Qué usuarios tienen los mismos permisos que el administrador?
- ¿La base de datos tiene suficientes recursos libres para trabajar?
- ¿Se borran físicamente los registros de las bases de datos cuando un usuario los elimina, o se marcan como "borrados"?

4.5. Control de aplicaciones

- ¿Todas las máquinas de la empresa tienen los mismos programas con las mismas versiones? ¿Existe un estándar de configuración de PC´s a seguir?
- ¿Usan alguna herramienta como el Norton Ghost para copiar la configuración de las PC's?
- ¿Existe un procedimiento para instalar las aplicaciones en las máquinas de los usuarios?
- ¿Quién los instala y administra?
- ¿Existen controles para realizar la instalación o la actualización de parches de las aplicaciones?
- ¿Cómo se documenta la instalación o actualización del software que se instala en las máquinas?
- ¿Existe algún procedimiento para encontrar programas que no deberían estar en las máquinas de los usuarios, ya sea por problemas de licencias o virus? ¿Existe un método a seguir? ¿Se usa algún producto para detectar estos programas? ¿Se hacen auditorias periódicas para verificar?
- ¿Cómo se controla a los usuarios y las aplicaciones que bajan de la web? ¿Cómo controlan que éstas tengan las licencias correspondientes (esto puede terminar en un problema para la empresa)? ¿Se borran las versiones de prueba (trial version) o demos cuando expiran?
- ¿Se permiten los registros on line de las aplicaciones?

- ¿Existen métodos para autorizar y registrar software?
- ¿Cómo manejan las actualizaciones del software?
- ¿Existe alguna forma de configurar las PC´s de manera que no se pueda instalar software nuevo sin autorización del administrador?
- ¿Puede pasar que un usuario no esté autorizado para modificar las carpetas c:\Windows o c:\Archivos de programa, pero otro (el administrador de sistemas) sí? ¿Cómo se configura esto en el sistema de control de acceso de la empresa? ¿Se usa?

4.6. Mantenimiento de aplicaciones

- ¿Cómo se etiquetan y almacenen los instaladores de los programas o los drivers? ¿Se almacenan en disco duro, en disquete, en CD, en cinta?
- ¿Existe algún tipo de mesa de reportes donde los usuarios con incidentes de seguridad pueden recibir ayuda o realizar un reporte?
- ¿Se controla el funcionamiento correcto de las aplicaciones? ¿Se hacen chequeos periódicos sobre el funcionamiento, la configuración, etc.? ¿Se generan alertas?
- ¿Cómo se administran las emergencias?
- ¿Si se hacen cambios de emergencia?, ¿cómo se documenta?
- ¿Se borran los archivos de las carpetas temporales, para que no se llenen los discos de basuras y provoquen la caída del sistema?
- ¿Se revisan periódicamente los sistemas para eliminar los programas o servicios innecesarios (como algunos servicios web, FTP, http)? ¿Se buscan vulnerabilidades nuevas durante estas revisiones?
- ¿Es automático el método de actualización de los Antivirus para que los mensajes internos en el interior y el exterior de la organización no propaguen virus? ¿Se programan los escaneos automáticos de virus una vez por semana? ¿Por qué no la actualiza la aplicación automáticamente con un schedule?
- ¿Existe alguna aplicación de gestión para tomar decisiones de alto nivel gerencial? ¿Esta obtiene datos automáticamente de las bases de datos?
- ¿Existe un undelete como la Papelera de Reciclaje de Norton? ¿En el servidor o en las PC´s?
- ¿Está habilitado el undelete de DOS?
- ¿Se hace un back up de la configuración de los sistemas antes de hacer algún cambio de manera de poder hacer un undo?

- ¿Los cambios complejos en los archivos de configuración se hacen primero (a modo de prueba) en una copia de los archivos o se hacen directamente en la configuración original?
- ¿Se registran o documentan los cambios hechos a una configuración?

4.7. Ciclo de vida

- ¿Qué aplicaciones se desarrollaron en la empresa? ¿Una para cada área de la empresa?
- ¿Qué metodología estándar usan para el desarrollo de sistemas? ¿De qué fases consta? ¿Qué mecanismos de seguridad manejan durante estas fases?

4.7.1. Iniciación

- ¿Cómo se expresan las necesidades del sistema?

4.7.2. Desarrollo

- ¿Se hace un análisis de riesgos antes de empezar con el desarrollo?
- ¿En caso de que haya participación de terceros en el desarrollo (como en la web, o en LINUX) el código fuente queda en la empresa? ¿Dejan documentación? ¿Tienen alguna reglamentación para trabajar con terceros?
- ¿Usan métricas durante el desarrollo? ¿Les sirven? ¿Qué miden? ¿En qué las utilizan?
- ¿Se mantienen registros históricos de las modificaciones llevadas a cabo en los sistemas durante el desarrollo y el mantenimiento? ¿Qué se guarda? sistema que afecta, fecha de la modificación, persona que realizó el cambio, descripción global de la modificación, ¿Qué más?
- ¿En qué momento se definen los requisitos de seguridad de un sistema? ¿Es durante el desarrollo?.

4.7.3. Implementación

- ¿En qué lenguajes se implementan los sistemas? ¿Reúsan software?
- ¿Qué medidas de seguridad toman durante la implementación?

4.7.4. Prueba

- ¿Cómo se hace la prueba de los sistemas?
- ¿Se generan planes de prueba?
- ¿Qué tipos de prueba se llevan a cabo? ¿De unidad? ¿De integración? ¿Por módulos? ¿Por sistema?

- ¿Se generan escenarios de prueba para el testeo?
- ¿Se documentan las pruebas y sus resultados? ¿Qué datos se guardan?
- ¿Cómo se realiza el control de cambios del sistema?

4.7.5. Instalación y mantenimiento

- ¿Qué metodología usan para el mantenimiento?

4.7.6. Documentación

- ¿Qué documentación generan de los desarrollos que hacen? ¿Se incluyen las siguientes cosas?
  - Generalidades del sistema, incluyendo fecha de implementación y analista / programador responsable.
  - Documentación del sistema, incluyendo sus objetivos, diagramas generales y de funciones y diseños de registros.
  - Documentación de los programas, incluyendo objetivos, diagrama de flujo y archivos de entrada y salida que utiliza.
  - Manual de operación, que contenga el diagrama de flujo general de procesamiento donde se identifiquen los procesos que deben haber finalizado y las interfaces de entrada que se deben haber cubierto como paso previo a la ejecución de cada proceso, los procedimientos de supervisión, seguridad y control sobre los procesos y los pasos a seguir ante la ocurrencia de errores.
  - Manual de usuario.
  - Manual de características de seguridad.
  - Descripción del hardware y software, políticas, estándares, procedimientos, backup, plan de contingencia, descripción del usuario y del operador del sistema.

4.7.7. Compra

- ¿Qué medidas se toman antes de comprar un sistema?
- ¿Cómo es el análisis que se hace?
- ¿Existe documentación de los sistemas comprados, así como los vendedores y del soporte postventa?

Anexo 5. Seguridad física

5.1. Control de acceso al centro de cómputos

- ¿Se hizo un análisis costo beneficio a la hora de implementar los controles? ¿Cómo se asesoraron?
- ¿Se restringe el acceso al centro de cómputos a la gente que no pertenece a esa área?
- ¿Existen algunos de los siguientes métodos? ¿Dónde? tarjetas de entradas, guardias de Seguridad, llaves Cifradas (Looked Door), circuito cerrado de televisión.
- ¿Cuál es la función de la doble puerta en la entrada?
- ¿Qué tipos de autenticación se utilizan en la empresa? Hay cuatro formas: con algo que el individuo sabe (password, PIN, etc.), algo que el individuo procesa (un token, una smart card, etc.), algo que el individuo es (controles biométricos), algo que sabe hacer (como los patrones de escritura).
- ¿Por qué no usan las otras? ¿Por el costo? ¿No vale la pena?
- ¿Solo dejan entrar a aquellos que lo necesiten? ¿Les hacen algún control de seguridad?

5.2. Control de acceso a equipos

- ¿Cómo se controlan los siguientes accesos?
- ¿El BIOS tiene habilitada una contraseña?
- ¿Las PC’s tienen habilitados los dispositivos externos, como la disquetera o la lectora de CD? ¿Cómo se controlan estos dispositivos?
- ¿Cómo se controlan los virus en las disqueteras o CD’s? ¿Qué otros peligros pueden tener?
- ¿Son dispositivos booteables (se permite desde el setup de la máquina el booteo con estos dispositivos)?
- ¿Ha habido robo de datos usando estos dispositivos?
- ¿Existen copiadoras de CD’s en la empresa? ¿Quién tiene acceso a ellas? ¿En qué máquinas están?
- ¿Usan llave de bloqueo en las CPU´s?
- ¿Las CPU´s y dispositivos externos extraíbles están guardados con llave?
- ¿Existe algún control sobre los terceros que realizan el mantenimiento?

- ¿Existen entradas no autorizadas en las PC's, como puertos no usados y no deshabilitados?
- ¿Puede alguien enchufar e instalar una impresora u otro dispositivo (un zip o un disco removible) en alguna máquina?
- ¿Cómo se realiza el control sobre los dispositivos que se instalan en las PC´s? ¿Se hace una revisión periódica de los mismos? ¿Quién las hace? ¿Cada cuánto? ¿Qué buscan?
- ¿Se apagan los servidores en algún momento? ¿Es necesario que queden prendidos las 24 hs?

5.3. Utilidades de soporte

- ¿Existen, se mantienen y revisan todos estos aparatos periódicamente en busca de fallas?

Aire acondicionado (18º C a 20º C)

Calefacción Humidificador en la biblioteca de cintas y centro de cómputos Luz de emergencia en el centro de cómputos Detectores de humo, agua y calor Instalación de alarmas:

- ✓ Contra fuego
- ✓ Humo
- ✓ Calor
- ✓ Intrusos
- ✓ Agua

- ¿Qué otras hay?

Servidor de repuesto o redundante

- UPS (Uninterruptible power supply) ¿para mantener los servidores de red funcionando por cuántas horas? ¿Cuántos UPS? ¿En qué máquinas?
- Estabilizador de tensión: ¿cuántos? ¿En qué máquinas?

Extinguidotes de incendio:

- ¿Son los adecuados?
- ¿Son manuales o automáticos (rociadores)?
- ¿Se corta la energía eléctrica cuando se activan estos rociadores?

- ¿Están en el lugar correcto? ¿En qué lugares? ¿Cómo eligieron el lugar?
- ¿Se revisan las posibles fallas eléctricas o posibles causas de incendio?
- ¿Qué pasa con las máquinas cuando cae la lluvia artificial? ¿Existen cubiertas plásticas para protección de agua?
- ¿Qué pasa con los extinguidores de incendio en el centro de cómputos?
- ¿Hay una sola red eléctrica?
- ¿Hay un dispositivo que evite la sobrecarga de la red eléctrica?
- ¿Hay hardware especial de aislamiento y protección de dispositivos magnéticos?

5.4. Estructura del edificio

- ¿Se tuvo en cuenta la seguridad de los datos y equipos en el momento de hacer la estructura de los edificios? ¿O se hizo primero la red y luego el edificio?

Centro de cómputos:

- ¿Está ubicado en pisos elevados (para prevenir inundaciones)?
- ¿Existe un piso o techo falso para pasar el cableado por debajo de él? ¿El área debajo del piso o del techo falso es fácilmente accesible?
- ¿Es lo suficientemente grande, anticipándose al crecimiento de la red y predispuesto a reinstalaciones?
- ¿La localización del centro de cómputos, tiene paredes externas o ventanas?
- ¿Está cera del (backbone) caño central de la red?
- ¿Está permitido comer, fumar y beber dentro del centro de cómputos?
- ¿En el resto de los escritorios se puede?

Cableado:

- ¿Usan cableado estructurado? ¿Quién lo instaló? ¿Tercer izaron la instalación?
- ¿Usaron alguna norma para hacer el cableado?
- ¿Se tuvo en cuenta el lugar de los canales de red, de manera que no sean afectados por desastres como inundación, cortes eléctricos, problemas de desagües o campos magnéticos?
- ¿Qué tipo de cable usan para que no haya interferencias?
- ¿Qué medidas toman para las interferencias?
- ¿Cómo previenen los daños o cortes en los cables?
- ¿Cómo calcularon el ancho de banda de la red? ¿Es suficiente?

- ¿Bocas de red: son suficientes? ¿Hay de más? ¿Cómo protegen a las que sobran? ¿Están habilitadas o no? ¿Cómo las deshabilitan?
- ¿Se conoce por donde van las cañerías de manera que no interfieran con la red?
- ¿El local se sitúa encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas?
- ¿Esto causa molestias o interferencias?
- ¿Existe un interruptor de energía de emergencia en la puerta de salida?
- ¿Los muebles son de madera? ¿Son inflamables?

5.5. Interceptación física, visual y electromagnética

- ¿Puede haber emisiones electromagnéticas desde los monitores o desde los cables UTP, que se pueden interceptar o provocar ruidos?
  - **Emisiones visuales:** ¿se evita que los monitores puedan verse a través de las ventanas?
  - **Emisiones de sonido (ruido):** ¿se toma alguna medida para que no afecten el funcionamiento normal? ¿Hay ruidos que puedan causar problemas? ¿La ubicación de las antenas de radio interfiere con los datos de alguna manera? ¿No son necesarias las cortinas de aluminio para aislar de ruido a las señales? ¿Usan algún otro tipo de aislamiento en algún lado?

5.6. Sistemas móviles

- ¿Si se usan laptops o PC's portátiles, se tienen en cuenta los diferentes riesgos a los que se someten los datos de la empresa?
- ¿Los dueños de las laptops son conscientes de la inseguridad que generan al tener datos sensibles en ellas? ¿Tienen en cuenta estos puntos?
- ¿Se encriptan los datos en un sistema móvil?
- ¿Se almacenan en lugares seguros los equipos móviles?
- ¿Las laptops tienen password de acceso?
- ¿Cómo se maneja el trabajo desde la casa?
- ¿Se hacen backups de los datos de los sistemas móviles? ¿Cómo y en qué medio?

5.7. Emergencias

- ¿Cómo se procede en caso de una emergencia?
  - Error físico de disco de un servidor, Error de memoria RAM, Error de tarjetas controladoras de disco, Incendio total o factores catastróficos, durante y

después de la situación de emergencia, ¿se controla el acceso al centro de cómputos?

5.8. Clasificación de datos y hardware

- ¿Existen procesos para rotular, manipular y dar de baja la computadora, sus periféricos y medios de almacenamiento removibles y no removibles? ¿Cómo son estos procesos? ¿Con qué se rotulan los dispositivos?
- ¿Tienen un inventario de recursos de hardware y software? ¿Existe documentación sobre los dispositivos instalados en cada máquina, su configuración, modificación, forma de mantenimiento, versión, etc.?
- ¿Cómo se guarda? ¿Es una planilla?
- ¿Dónde se almacena?
- ¿Quién lo actualiza?
- ¿Cada cuánto?

5.9. Backup

- ¿Con qué frecuencia hacen los backups?
- ¿Qué datos se almacenan? (datos y programas de aplicación y de sistemas, equipamiento, requerimientos de comunicaciones, documentación)

Software de base y su configuración:

- ¿Se hacen discos de inicio de Windows?
- ¿Hay imágenes Ghost de las máquinas?
- ¿Se hacen backups de la configuración de red?
- Software aplicativo, Parámetros de sistema, Logs e informes de auditorías, Datos, ¿Qué más?

Backups del Hardware.

- **Modalidad externa:** ¿contratan un tercero que proporcione los insumos necesarios en caso de emergencia?
- **Modalidad interna:** si tienen más de un local, en ambos locales saben tener señalados los equipos, que, por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local. ¿Se realizan estas actividades en la empresa?

- Radio: ¿si se cae un nodo de la radio, que pasa? ¿Hay algún servicio técnico o de respaldo para esto?
- ¿Hay backup especiales (con datos distintos, o particulares)? ¿Cada qué período de tiempo se hacen? ¿Qué datos guardan? ¿Qué tipo de back up hacen? (backups normales, backups incrementales, backups diferenciales) ¿En qué áreas o datos usan incrementales, en cuáles usan normales, etc.? ¿En qué medio se almacena? ¿Con qué dispositivo se hace? ¿Cómo es la rotación de los medios de backup? ¿En una semana, un mes?
- ¿Con qué aplicación se hacen? ¿Con algún tipo especial de aplicación de manejo de backup? ¿Es una del sistema operativo, del administrador de archivos u otra? ¿Utilizan archivos de tipo específicos o archivos? ¿zip, por ejemplo?
- ¿Hay herramientas de back up automáticas, o sea que a través de una agenda hacen las copias?
- ¿Quién es el encargado o el responsable? ¿Los hace el administrador de sistemas?
- ¿Tienen formalizados los procedimientos de back up? ¿Existe un procedimiento escrito? ¿Si falta el responsable del backup, quién los hace?
- ¿Existen procedimientos escritos para recuperar archivos backupeados, o un Plan de backup?
- ¿Hacen pruebas periódicas de recuperación de backups?
- ¿Quién puede levantar los archivos de los usuarios, los backups de Mis ¿Documentos, cualquier otro usuario?
- ¿Qué PC's o máquina es la que tiene mayor prioridad? ¿Cómo son las prioridades? ¿Según qué se determinó la prioridad de las máquinas: según un análisis de impacto, ¿según la confidencialidad de la información? ¿Los backups se almacenan dentro y fuera del edificio? ¿Estos lugares son seguros?
- ¿Cómo se rotulan e identifican?
- ¿Hay documentación escrita sobre los backups hechos, sus modificaciones, fechas, etc.?
- ¿Se necesita algún dispositivo (llaves, tarjeta) para entrar al almacén de cintas?
- ¿Se crean discos de inicio de Windows?
- ¿Hay información afuera de la red interna de la empresa que sea valiosa? ¿El web host tiene datos importantes de usuarios? ¿Se hacen backups de estos datos? ¿Dentro de la empresa o por el web host?

- ¿Hay backups de las páginas web y de sus actualizaciones?
- ¿Existen procedimientos automáticos para que, en caso que un usuario cometa un error en la base de datos, ésta pueda volverse a su estado anterior? ¿Cómo se hace?

Anexo 6. Administración del centro de cómputos

6.1. Countermeasures del CPD

- ¿Se realizan los siguientes chequeos en el sistema?

Diariamente:

- ¿Extraen un logístico sobre el volumen de correo transportado?
- ¿Extraen un logístico sobre las conexiones de red levantadas? Semanalmente
- ¿Extraen un logístico sobre los intentos de ingresos desde el exterior a la red interna?
- ¿Extraen un logístico con las conexiones externas realizadas desde nuestra red?
- ¿Obtienen un logístico sobre los downloads de archivos realizados y quién los realizó?
- ¿Obtienen gráficos sobre tráfico en la red?
- ¿Obtienen logísticos sobre conexiones realizadas en horarios no normales (desde dónde, a qué hora y con qué destino)? Mensualmente ¿Realizan un seguimiento de todos los archivos logísticos a fin de detectar cambios en las estadísticas obtenidas (realizados en comparación con los archivos del mes anterior, por ejemplo)?
- ¿Existe un programa que haga estas comparaciones? ¿Se usa? ¿Da buenos resultados? ¿Existen procedimientos para dar publicidad a las nuevas normas de seguridad? ¿Cómo harían el aviso de las políticas de seguridad?
- ¿A través del mailing?
- ¿Con charlas o reuniones?
- ¿Exposición en transparencias?
- ¿Por una notificación expresa a cada empleado?
- ¿Cómo funciona el boletín mensual que les entregan a los usuarios? ¿Qué temas trata? ¿Se entrena a los usuarios y administradores? ¿Quién es el encargado? ¿Por qué? ¿Se tienen en cuenta los delitos no tecnológicos? (Ej: discutir temas privados de la organización en lugares no aptos, ingeniería social, etc.) ¿Existe algún tipo de mesa de reportes donde los usuarios con incidentes de seguridad pueden recibir ayuda o realizar un reporte? ¿Existe un tipo de feedback o buzón de sugerencia de cambios de los usuarios? ¿Existe un Plan de Sistemas formal? (plan a corto plazo de actividades del CC)

- ¿Quién los hace?
- ¿En base a qué estudios definen las cosas por hacer?
- ¿Existe un Plan Estratégico de Sistemas? (plan a largo plazo de proyectos) ¿Existen políticas, normas, estándares y procedimientos que sirvan como base para la planificación, el control y la evaluación de las actividades del área de sistemas de información?
- ¿Existe una planificación y documentación escrita y actualizada de las actividades que se desarrollan normalmente en el centro de procesamiento de información? Deberá incluir como mínimo el detalle de:
  - ✓ Los procesos a realizar,
  - ✓ Los controles que se efectúan,
  - ✓ Los mecanismos de registros de problemas y hechos,
  - ✓ Los procedimientos sobre cancelaciones y re-procesos en cada una de las actividades,
  - ✓ Las relaciones con otras áreas,
  - ✓ Los mecanismos de distribución de la información.
- ¿Existe documentación detallada sobre el equipamiento informático? ¿Incluye los siguientes datos? distribución física de las instalaciones (identificación de PC´s y equipos, y puesto de trabajo),
- inventario de "hardware" y "software" de base, número de serie de hardware, número de licencia de software, inventario de insumos, diagramas topológicos de las redes, tipos de vínculos, ubicación de nodos, trabajos de mantenimiento y entrada del personal externo.
- ¿Se tienen en cuenta tanto al centro de procesamiento de datos principal como de los secundarios, redes departamentales, sucursales y al centro alternativo para contingencias? ¿Se actualiza la lista de activos?
- ¿Existe algún manual de seguridad, para el personal de seguridad o para los usuarios? Existe alguno de los siguientes documentos:
  - ✓ Plan de contingencia
  - ✓ Plan de continuidad
  - ✓ Plan de seguridad
  - ✓ Manual de procedimientos del CPD

Trusted Facility Manual: detalla las funciones y privilegios de la seguridad. Contiene: configuración, administración y operación del sistema, guías para el buen uso de las características de protección del sistema, etc.

Security Features User's guide: asiste a los usuarios del sistema, describe cómo usar las protecciones, las responsabilidades de la seguridad del sistema.

- ¿Es automático el método de actualización de los antivirus para que los mensajes internos en el interior y el exterior de la organización no propaguen virus? ¿Se programan los escaneos automáticos de virus? ¿Cada cuánto tiempo? ¿Por qué no se actualiza la aplicación automáticamente con un schedule?
- ¿Cómo se etiquetan y almacenen los instaladores de los programas o los drivers? ¿Se almacenan en disco duro, en disquete, en CD, en cinta?
- ¿Se borran los archivos de las carpetas temporales, para que no se llenan los discos de basuras y provoquen la caída del sistema?
- Todas estas tareas ¿Son realmente útiles? ¿Se dan en la práctica?

6.2 Responsabilidad del equipo de seguridad

- ¿Cómo se administran las emergencias? ¿Si se hacen cambios de emergencia, cómo se documenta?
- ¿Quién es el encargado de la seguridad? ¿Y de una política de seguridad y su administración?
- ¿Quién se encarga de administrar la estructura de seguridad una vez implementada?
- ¿Existe un solo responsable del centro de cómputos?
- ¿Qué privilegios (o accesos) se les dan a las personas recién contratadas en el centro de cómputos?
- ¿Cuál es la diferencia de permisos entre los desarrolladores y los administradores?
- ¿Quién asigna los permisos a los distintos roles o grupos?
- ¿Quién es el encargado de informar a los ejecutivos de la empresa sobre la administración de seguridad, actividad de seguridad de la información, y riesgos? ¿Se realizan informes periódicos? ¿Son a pedido de alguien o a modo de auto evaluación?

- ¿Quién es el encargado de recomendar la separación de tareas y responsabilidades para las funciones de IT?
- ¿Quién es responsable de asegurar que los sistemas de seguridad física están en su lugar?
- ¿Existe en los empleados y altos ejecutivos una conciencia sobre su importancia de la seguridad?
- Todas estas tareas ¿Son realmente útiles? ¿Se dan en la práctica?

Anexo 7. Auditorías y revisiones

7.1. Auditorías generales

- ¿Se hacen auditorías en la empresa?
- ¿Qué objetos se auditan? Para cada clase de objetos, ¿qué accesos se auditarán?
  - Archivos y directorios
  - Claves del registro
  - Servicios
  - Objetos del kernel
  - Impresoras
- ¿Qué actividades se monitorizan?
  - Monitorización del sistema general
  - Monitorización de reinicio de los sistemas
  - Monitorización de colapsos (crashes) del sistema
  - Monitorización de fallas de hardware
  - Monitorización de procesos
  - Monitorización de aplicaciones
- Gestión de red: ¿Para el monitoreo de la red se utilizan aplicaciones propias de Linux, como:
  - ¿Monitores de tráfico de red?
  - ¿Monitores de rendimiento?
  - ¿Monitores de control de cantidad de archivos abiertos?
  - ¿Monitores de usuarios conectados al servidor?
  - ¿Aplicación de monitoreo gráfico de la red?
- ¿Qué otra clase de eventos se auditarán?
- ¿Con qué tipo de herramientas se hace la monitorización?
  - ✓ Escáner de puertos y vulnerabilidades
  - ✓ Chequeadores del sistema de archivos
  - ✓ Analizadores de logs de eventos
  - ✓ Analizadores de registro
  - ✓ Analizadores de listas de control de acceso (ACL)

  Sniffers de paquetes

  Herramientas para craquear passwords

Escáner de seguridad integral (Overall security scanners)

- ¿Se hacen chequeos aleatorios para verificar el cumplimiento de los requerimientos y procedimientos de seguridad? ¿Sería útil?
- ¿Cuánto se monitoriza? (Monitorizar tiene un impacto directo en la performance del sistema) ¿Cómo hacen para que los recursos alcancen? ¿Cómo hacen con cada uno de los cuellos de botella?
  - ✓ Carga de CPU
  - ✓ Memoria disponible
  - ✓ Performance del sistema de disco
  - ✓ Ancho de anda de la red
- ¿Cuándo se eliminan los logs para evitar llenar el disco? ¿Tienen un tamaño máximo?
- ¿Qué pasa con la información que se obtiene de las auditorías? ¿Pasa algo de lo siguiente?

Se solicita la información y se ve que:

- ✓ No tiene y se necesita.
- ✓ No se tiene y no se necesita.
- ✓ Se tiene la información, pero:
- ✓ No se usa.
- ✓ Es incompleta.
- ✓ No está actualizada.
- ✓ No es la adecuada.
- ✓ Se usa, está actualizada, es la adecuada y está completa.

- ¿Las auditorías permiten rastrear las acciones de cada usuario? ¿Que se audita? ¿Se audita según las acciones, las maquinas o los usuarios?
- ¿Cada uno de estos activos en particular o depende de los sectores y/o máquinas y/o sensibilidad de la información?
- ¿Las auditorías soportan investigaciones luego de los hechos, con datos sobre cómo, ¿cuándo y por qué cesaron las operaciones normales?
- ¿Se reúne información de las auditorías para formar perfiles de los usuarios del sistema? ¿Observan, por ejemplo, patrones en los usuarios, como las terminales

que utilizan, horas de acceso, y permisos que solicitan, para determinar qué acciones son inusuales y deben ser investigadas?

- ¿Se usan herramientas automáticas para revisar los registros de auditorías en tiempo real?
- ¿Debido a que no hay herramientas que generen warnings ni alarmas, se revisan los logs de auditorías periódicamente? ¿Qué se revisa? ¿La aplicación es en tiempo real?
- ¿La aplicación es del sistema operativo, es un programa desarrollado por ustedes o es un programa comprado?
- Se deberían utilizar chequeos aleatorios, con frecuencias más bajas, para hacer auditorios manuales y/o mensuales de este tipo.
- ¿Se generan históricos de auditoria indicando qué procesos se corrigieron, quién los corrigió y qué cambios hizo (control de cambios gestión de configuración)?
- ¿Se investiga la actividad sospechosa? ¿Se toman acciones? ¿Se documentan la ejecución y los resultados de estas pruebas?

7.2. LOGS:

- ¿Está controlado el acceso a los logs on line de auditoria?
- ¿Cómo se identifica qué tipo de logs son generados? ¿Se almacenan en diferentes carpetas los que son generados por diferentes programas?
- ¿Los logs se almacenan externamente a la empresa? ¿Los almacenamientos externos de logs de auditorías se retienen por un período de tiempo? ¿Está controlado el acceso a estos logs, también?
- ¿Hay demasiada información guardada? ¿Los archivos largos de logs hacen más difícil encontrar irregularidades?

Los logs de los eventos deberían contener los siguientes campos:

- ✓ Fecha y hora
- ✓ Tipo (severidad del evento)
- ✓ Fuente (el componente que disparó o logeo el evento)
- ✓ Categoría (subgrupo de eventos de seguridad)
- ✓ ID del evento (número único que identifica el evento)
- ✓ Usuario (nombre del usuario relacionado con el evento, si hay)
- ✓ Computadora (máquina donde se logeo el evento)

- ✓ Descripción (datos como mensajes de error, asociados con el evento)
- ✓ Datos (datos binarios asociados con el evento)

Análisis de los logs de auditoria:

- ¿Qué datos son los más importantes o los más leídos?
- ¿Cuánto tiempo lleva hacer los análisis?
- ¿Es necesario mejorar los análisis? ¿De qué forma, cuál es la falla?
- ¿Porque no se analizan los logs, aunque sea los que posean alguna conducta irregular?
- ¿Es totalmente necesario un sistema automático de monitorización y análisis de logs que emita alarmas ante determinados eventos? ¿Porque esto no se da en la realidad? ¿Es mucho trabajo?
- ¿No vale la pena? ¿No hay gente que se dedique a esto?

7.3. Línea de base

- ¿Se hace una línea de base de la performance de los servidores y de la red? ¿Qué medidas se toman?
- ¿Qué datos se recogen para hacer la línea?
- ¿A qué intervalo de tiempo se toman estos datos? ¿Con qué frecuencia se tomarán las líneas base?
- ¿Se hacen nuevamente las líneas de base si se modifica alguna configuración en el sistema?
- ¿Cuándo se actualizan las líneas de base?
- ¿Cómo se guardan? ¿Dónde? ¿En qué formato?

7.4 Responsabilidades de los encargados de seguridad

- ¿Quién administra, desarrolla e implementa los procedimientos de auditoría y revisión? ¿Quién conduce la auditoría?
- ¿Quién selecciona los eventos de seguridad a ser auditados?
- ¿Quién administra la documentación sobre los resultados?
- ¿Quién se encarga de monitorizar y reaccionar a los avisos (warnings) y reportes?
- ¿Quién hace chequeos aleatorios para verificar el cumplimiento de los requerimientos y procedimientos de seguridad?

- ¿Quién se encarga de reunir datos de las auditorías para formar perfiles de los usuarios del sistema?
- ¿Quién revisa los reportes de auditorías buscando anomalías?
- ¿Hay separación de tareas entre los que administran el control de acceso y los que hacen las auditorías, o son las mismas personas?
- ¿Quién se encarga de buscar nuevas herramientas que faciliten la auditoría?

7.4. Auditorías del servidor

CPU del servidor usado

- ¿Qué trabajos usan más CPU?
- ¿Quién usa más CPU?
- ¿En qué momento se usa más el CPU?
- ¿Cuánto tiempo el CPU permanece usada en un 100?

Memoria del servidor usada

- ¿Qué trabajos usan más memoria?
- ¿Quién usa más memoria?
- ¿En qué momento se usa más la memoria?
- ¿Cuánto tiempo la memoria permanece usada en un 100?

Datos del servidor usados

- ¿Qué datos son los que consumen más tráfico, memoria o CPU?
- ¿Qué datos se usan más?
- ¿Qué datos se modifican más?
- ¿Quién entra a cada dato?
- Aplicaciones del servidor usadas
- ¿Qué aplicaciones consumen más recursos?
- ¿Qué aplicaciones se usan más?

7.5. Auditorías de control de acceso

- ¿Se generan logs de auditoria del control de acceso?
- ¿Cuándo se almacenan, ante qué eventos? ¿Se almacenen cuando ocurre alguno de estos eventos?
  - ✓ Login exitoso

- ✓ Login fallido
- ✓ Procedimientos de cambios de passwords satisfactorio
- ✓ Procedimientos de cambios de passwords fallido
- ✓ Lockeo de un usuario
- ✓ Modificación en bases de datos
- ✓ Utilización de herramientas del sistema
- ✓ Modificación de ciertos datos (como datos de configuración, datos críticos, datos de otros usuarios)
- ✓ Acceso a Internet
- ✓ Alertas de virus

- ¿Dónde se almacenan?
- ¿Quién tiene acceso a los logs?
- ¿Por cuánto tiempo permanecen guardados?
- ¿Se borran cuando expira ese tiempo o se genera una estadística comprimida de los mismos y de guarda un análisis de ellos solamente? ¿Qué datos se almacenan en los logs? ¿Se almacenan los siguientes datos?

Para todos los eventos:

- ✓ Fecha y hora del evento
- ✓ Tipo de evento (Ej. Login, modificación de datos, etc.)
- ✓ ID de usuario
- ✓ Origen del evento (Ej. Terminal Nº 9)

Acceso a Internet:

- ✓ Páginas visitadas
- ✓ Cookies guardadas
- ✓ Archivos descargados
- ✓ Servicios utilizados
- ✓ Aplicaciones utilizadas
- ✓ Modificación de ciertos datos
- ✓ Datos modificados

- Valor anterior - ¿por cuánto tiempo se guarda el valor anterior de los datos? ¿Se hace alguna comprobación antes de efectuar el cambio definitivo?

- ¿Qué se hace si se modifica algún valor de la configuración del sistema?
  - ✓ Login fallido
  - ✓ Motivo del fallo
  - ✓ Procedimientos de cambios de passwords
  - ✓ Password anterior
  - ✓ Password nueva fallida
  - ✓ Aplicación usada
  - ✓ Motivo del fallo
  - ✓ Lockeo de un usuario
  - ✓ Motivo del lockeo del usuario
  - ✓ Aplicación que realiza el lockeo.
  - ✓ Modificación en bases de datos
  - ✓ Datos modificados
  - ✓ Valor anterior
  - ✓ Aplicación usada
  - ✓ Utilización de herramientas del sistema
  - ✓ Herramienta usada
  - ✓ Rastreo de acciones del usuario con esa herramienta
  - ✓ Modificaciones realizadas.
- ¿Las estadísticas que genera son buenas? ¿Faltan datos por analizar que son importantes para la administración del control de acceso?
- Prestar especial atención con los logs que fueron generados con el ID de administrador, ¿hay irregularidades en estos logs? ¿Se han controlado alguna vez?

7.6. Auditorías de redes

7.6.1. Correo:

- ¿La herramienta de administración de correo genera logs de auditoria?
- ¿Qué contienen?
- ¿Quién los administra?
- ¿Cada cuánto se leen?
- ¿Se generan avisos cuando:
- ¿Se está por llenar el espacio asignado para el correo?
- ¿Hay muchos mensajes es de la misma dirección fuente?
- ¿Hay muchos mensajes es para la misma dirección destino?

- ¿Hay muchos mensajes con el mismo encabezado, o cuerpo, o archivo adjunto?
- ¿Hay posibles virus?
- ¿Hay SPAM? ¿Se baja la performance del correo?
- ¿Hay algún problema para enviar o recibir los mensajes?
- ¿Hay muchos mensajes es entrantes o salientes, más de lo normal? ¿Cuándo más?

7.6.2. Mantenimiento - Monitoreo - Auditorias

- ¿Usan herramientas de monitorización de red?
- ¿Se hace algún chequeo periódico de la red y sus permisos?
- ¿Qué datos se pueden ver? Datos
- ¿Programas que se ejecutan en las PC's y servidores?
- ¿Qué prioridades tienen los trabajos?
- ¿Qué prioridades tienen los usuarios?
- ¿Con qué reglas de trabajos se están corriendo?
- ¿El estado de cada trabajo (en cola, ejecutándose, esperando una respuesta del operador, etc.)?
- ¿Desde dónde se ejecuta el programa (usuario, ¿ID, terminal)?
- ¿Porcentaje de CPU y memoria (recursos) usado por programa? ¿Y por terminal? ¿Y por usuario?
- ¿Colas de impresión de cada usuario? ¿De cada impresora? ¿De cada terminal?
- ¿Trabajos programados por cada usuario? ¿Por cada terminal?
- ¿Dispositivos conectados a la red? ¿El estado de los dispositivos?
- ¿Dispositivos con problemas?
- ¿Qué usuario está asignado (o usando) cada dispositivo? ¿Qué trabajo lo está ocupando?
- ¿Se monitorean los puertos de la red? ¿Se puede ver si hay intentos de intrusión?
  - Alertas de virus - Tipo y nombre del virus Archivo infectado (nombre, ubicación etc.)
  - Antivirus usado Acciones llevadas a cabo Resultado de las acciones (satisfactorio o no).

Estadísticas de red:

- ¿En qué parte de la línea el tráfico es más intenso?

- ¿Quién de las terminales usa más tráfico de red?
- ¿Gráfico del uso de la red por terminal?
- ¿Se discrimina el tráfico ocupado por mail, datos, aplicaciones, mensajes, Internet, etc.?
- ¿Cuantos intentos de intrusos hubo?
- ¿Cuantos intentos de otros ataques? Etc.

Internet

- ¿Páginas más visitadas por usuario?
- ¿Tiempo promedio de estadía en Internet?
- ¿Recursos usados por Internet?

Mail

- ¿Cantidad de datos que se mueven diariamente vía mail? ¿Mensualmente? ¿Anualmente?
- ¿Cantidad de mail enviados y recibidos por usuario? ¿Por departamento? ¿En toda la empresa?
- ¿Controles para saber si un usuario en particular excede el promedio de mail diarios?
- ¿Mensajes infectados, salientes y entrantes?
- ¿Se usan estadísticas para controlar el mail bombing?

Virus

- ¿Cantidad de mails infectados en un determinado tiempo?
- ¿Direcciones fuentes qué más mails infectados envía?
- ¿Cantidad de archivos infectados por extensión? (Ej. Los archivos de Word se infectan más que los de Excel).

Alarmas - Avisos

- ¿Se generan avisos ante virus?
- ¿Se generan avisos ante intrusos?
- ¿Se generan avisos ante poco espacio en disco de servidores o de PC’s?

- ¿Se generan avisos ante poca disponibilidad de CPU o de memoria en los servidores?
- ¿Cuándo más?

- ¿Quién se encarga de procesar y/o monitorear los datos generados por la herramienta? ¿Cómo se actúa en consecuencia? ¿Existe algún procedimiento específico? ¿Qué datos parecen faltar al monitor de red que serían útiles para la administración de la red?

Anexo 8. Plan de contingencias

8.1. Plan de contingencias

- ¿Existe un plan de contingencias? ¿Cómo es? ¿Es formal? ¿Quién lo desarrolló? ¿Ha habido alguna contingencia que justifique el desarrollo del plan?
- ¿Se desarrolló un previo análisis de riesgo antes de realizar el plan de contingencias?
- ¿El plan de contingencias se desarrolló solo en base al área de cómputos, o se tuvieron en cuenta otras áreas de la empresa? ¿Cuáles? ¿Por qué esas áreas?
- ¿El plan de contingencias incluye un Plan de recuperación de desastres?
- ¿El plan de contingencias incluye un Plan de reducción de riesgos?
- ¿Se definen las responsabilidades y funciones de las personas en el plan de contingencias?
- ¿Existe entrenamiento para los responsables del plan de contingencias? ¿Y para los usuarios?
- ¿Poseen las acciones defensivas en caso de violación interna o externa? (Ej. desconectar los servidores, cerrar los accesos, rastrear al intruso, etc.), ¿Hay algún tipo de mecanismo de reportes o historial, para el manejo de incidentes?
- ¿Documentan el plan de contingencias? ¿Contiene todos estos datos?:
  - ✓ Objetivo del plan.
  - ✓ Modo de ejecución.
  - ✓ Tiempo de duración.
  - ✓ Costes estimados.
  - ✓ Recursos necesarios.
  - ✓ Evento a partir del cual se pondrá en marcha el plan.
  - ✓ Personas encargadas de llevar a cabo el plan y sus respectivas responsabilidades.
- ¿Existe alguna copia del plan de contingencia fuera de la empresa? ¿Está protegida en caja de seguridad? ¿Cada cuánto se actualiza?
- ¿Se hacen pruebas del plan? ¿Con qué frecuencia? ¿Anualmente?
- ¿Se mantiene actualizado de acuerdo a nuevos puestos y funciones, o amenazas?.

8.2. CPD alternativo

- ¿Se mantiene un centro de procesamiento alternativo? ¿Qué características tiene, en comparación con el CPD principal?
- ¿Es propio o contratan un tercero que facilite el CPD? En el segundo caso, ¿cómo es el contrato para este servicio?
- ¿Cómo se aseguran que este centro tenga las mismas condiciones de seguridad y calidad que las instalaciones del CPD principal?
- ¿Existe la posibilidad de poner el CDP alternativo en otra sucursal o en otro lado? ¿Por qué?
- ¿Si llega a haber un problema, en cuanto tiempo puede estar en óptimo funcionamiento este CPD alternativo?

8.3. Plan de recuperación de desastres

- ¿Cuánto cuesta un plan de recuperación de desastres? ¿Tiene relación con la información a recuperar? ¿O a cualquier costo se salva la información crítica? ¿En el caso de que haya un plan, cada miembro del equipo tiene una responsabilidad asignada? ¿O la responsabilidad es del Departamento de Sistemas? ¿Se dividen las acciones correctivas en equipos de trabajo? ¿Cómo
- ¿Forman esos equipos? ¿Dependen del desastre ocurrido? ¿Luego del desastre existe un equipo de evaluación para corregir y documentar los errores cometidos en tal circunstancia, para luego generar un plan de contingencia de mayor efectividad y eficiencia?

8.3.1. Antes del desastre

Identificación de las funciones críticas.

- ¿Cuáles serían los datos críticos a proteger en la organización, en el momento de un desastre? (Agregar lista de datos).
- ¿Cuáles serían los elementos de hardware y de software críticos a proteger en la organización, en el momento de un desastre? (Agregar lista de elementos).
- ¿Cómo se ordenarían según la importancia? Constitución del grupo de desarrollo del plan.
- ¿Quién sería el responsable del plan de emergencias, de su implementación y puesta en práctica? ¿El Jefe de Sistemas?

- En cada área que cubrirá el plan debe haber un líder del plan de contingencia. ¿Quién sugiere, el Jefe de cada área? ¿Alguien de más bajo rango? ¿Por qué?

Sistemas de información:

- ¿Existe un responsable de la información, en cada área de la empresa? ¿Conocen sus responsabilidades? ¿Los responsables que figuran en la documentación, son los que ejercen realmente el papel de responsables de la información? ¿Qué funciones tiene que cumplir?
- ¿Están identificados todos los sistemas de información y sus características (como si fuera un inventario de los sistemas)?
- ¿Qué datos se almacenan de los sistemas? Se sugiere almacenar:
  - ✓ Nombre
  - ✓ Lenguaje
  - ✓ Departamento de la empresa que genera la información (dueño del sistema)
  - ✓ Departamentos de la empresa que usan la información
  - ✓ Volumen de archivos con los que trabaja
  - ✓ Volumen de transacciones diarias, semanales y mensuales que maneja el sistema
  - ✓ Equipamiento necesario para un manejo óptimo del Sistema La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.
  - ✓ El nivel de importancia estratégica que tiene la información de este Sistema para la Institución (medido en horas o días que la Institución puede funcionar adecuadamente, sin disponer de la información del Sistema).
  - ✓ Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para que el equipamiento sea el mínimo posible).
  - ✓ Actividades a realizar para volver a contar con el Sistema de Información (actividades de restauración).
- ¿Se puede dar un orden de importancia a los sistemas de la lista de arriba?

Equipos de cómputos:

- ¿Se mantiene un inventario de los equipos de cómputos? Se debería incluir:

- Hardware: procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, routers, bridges.
- Software: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones.
- Datos (principales archivos que contienen los equipos): durante la ejecución, almacenados en línea, archivados fuera de línea, back-up, bases de datos, dueño designado de la información.
- Configuración de los equipos (y sus archivos de configuración).
- Ubicación de los equipos y de los datos. Nivel de uso Institucional de los equipos. Etc.
- ¿Existen pólizas de seguros para los equipos en el caso de siniestros? ¿Cómo son estos seguros?
- ¿Las PC’s o equipos se categorizan según su importancia (¿señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación?
- ¿Existe una relación de las PC's requeridas como mínimo para cada ¿Sistema permanente de la Institución? ¿Está actualizada siempre?

Backup:

- ¿Existen procedimientos para realizar back up? ¿Están incluidos en el plan de contingencia?
- Definición de los niveles mínimos de servicio. ¿Cuáles son las contingencias o problemas que pueden ocurrir? (agregar lista de las posibles contingencias)
- ¿Cuáles serían los peores problemas a los que se puede ver sometida la empresa? ¿Cuáles serían las peores contingencias?
- ¿Cuáles serían las más probables?
- ¿Cuáles son las que ocurren más a menudo?
- ¿Cuáles son las que no ocurren nunca? - ¿Se pueden nombrar algunas funciones o servicios que funcionen como los niveles críticos de servicio para cada una de las contingencias nombradas arriba? ¿Qué opinión tiene el jefe de cada área en cuanto a los niveles críticos de su área? Un ejemplo puede ser: el que no se caiga el servidor de aplicaciones, o el router, o la conexión de radio.

- ¿Qué recursos se necesitan para que funcione este servicio?
- ¿Cuáles son las prioridades de procesamiento que tendrán estas funciones o servicios críticos en caso de una emergencia?
- Evaluación de la relación coste / beneficio de cada alternativa.
- ¿Qué costo tendría cada uno de los niveles críticos de servicio que se determinaron arriba? Contar los costos de implementación, de mantenimiento, de entrenamiento de usuarios, y de restauración en caso de una emergencia.

Entrenamiento:

- ¿Entrenan al personal de alguna manera ante un siniestro?
- ¿Simulan siniestros para entrenar al personal?

8.3.2. Durante el desastre

- ¿Poseen un plan de emergencia (consiste de las acciones a llevar a cabo durante el siniestro)?
- ¿Se tienen en cuenta los distintos escenarios posibles? Ej.: durante el día, la noche.
- ¿Se incluyen los siguientes puntos?: ¿Vías de salida? ¿Plan de evacuación del personal?
- ¿Plan de puesta a buen recaudo de los activos? ¿Ubicación y señalización de los elementos contra el siniestro?
- ¿Existen funciones (encargado de retirar los equipos, encargado de las cintas, etc.) y equipos con funciones claramente definidas a ejecutar durante el siniestro?

8.3.3 Después del desastre

- Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el Plan de Acción Evaluación de Daños: ¿se realizan las siguientes actividades después de que ha ocurrido algún desastre?
- ¿Evalúan la magnitud del daño que se ha producido? ¿Qué sistemas se están afectando?
- ¿Qué equipos han quedado no operativos? ¿Cuáles se pueden recuperar? ¿En cuánto tiempo?
- ¿Qué más se evalúa o debería evaluarse, según sus experiencias?

Ejecución de Actividades.

- ¿Se determina un coordinador que se encargará de las operaciones necesarias para que el sistema funcione correctamente, después de la emergencia? Para cada tipo de emergencia, de las enumeradas arriba, ¿qué acciones se deben tomar para que el sistema vuelva a su funcionamiento normal?

Evaluación de Resultados.

- ¿Se evalúan los desempeños de las personas, y del Plan, luego de ocurrido el desastre? ¿Se genera una lista de recomendaciones para minimizar los riesgos?

Retroalimentación del Plan de Acción.

- ¿Se evalúa el desempeño del personal durante el desastre? ¿Se tiene en cuenta la información que se obtiene luego de una emergencia para retroalimentar el Plan?
- ¿Se reordena la lista de personal afectado en tareas de emergencia, con esta experiencia obtenida?
- ¿Se modifican las prioridades? ¿Qué elemento tenía demasiada prioridad? ¿Qué actividades faltaron incluir en el plan de emergencia? ¿Qué se mejoraría?
- ¿Cuál hubiera sido el costo de no haber tenido el plan de contingencias? ¿Qué se hubiera perdido?