UNIVERSIDAD NACIONAL DE MOQUEGUA

FACULTAD DE INGENIERIA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

INFORME DE EXAMEN PROFESIONAL

INFORME DE AUDITORIA, APLICANDO LA NTP/ISO 17799, CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA SUBREGIÓN ILO

PRESENTADO POR:

BACH. JUSSARA MILAGROS ARANGO RODRIGUEZ

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMATICA

MOQUEGUA – PERÚ

2022

UNIVERSIDAD NACIONAL DE MOQUEGUA

FACULTAD DE INGENIERIA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

INFORME DE EXAMEN PROFESIONAL

INFORME DE AUDITORIA, APLICANDO LA NTP/ISO 17799, CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA SUBREGIÓN ILO

PRESENTADO POR:

JUSSARA MILAGROS ARANGO RODRIGUEZ

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMATICA

_____

BACH. JUSSARA MILAGROS ARANGO RODRIGUEZ

_____

MSC. José Antonio Guzmán Valdivia

ASESOR

MOQUEGUA - PERÚ

2022

UNAM
UNIVERSIDAD NACIONAL DE MOQUEGUA

UNIVERSIDAD NACIONAL DE MOQUEGUA
FEDATARIO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Folio Nº 023

ACTA DE TITULACIÓN

I. Modalidad:
Examen Profesional

II. Documento de aprobación:
Resolución de Comisión Organizadora Nº 636-2022-UNAM
Fecha: 19 de agosto de 2022

III. Título de Informe de Examen Profesional:
Informe de Auditoria, aplicando la NTP/ISO 17799, código de buenas prácticas para la gestión de la seguridad de la información en la Subregión Ilo.

Bachiller: Jussara Milagros Arango Rodriguez
Asesor Principal: Mgi. José Antonio Guzmán Valdivia
Co-Asesor: .....

IV. Se dictamina con las siguientes notas:

Examen Escrito: 12.40 Entrevista: 2.80 Promedio: 15

Promedio en letras: Quince por lo que: Sí [X] No [ ]

Opta el Título Profesional de INGENIERO DE SISTEMAS E INFORMÁTICA.

Siendo las 10:13 horas, del 24 de octubre del año 2022 se procede con la firma en conformidad de lo dictaminado.

MSc. Hugo Euler Tito Chura
Presidente del Comité de Grados y Títulos
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

M.Sc. Victor Yana Mamani
Director
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Mgi. José A. Guzmán Valdivia
Asesor
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Bach. Jussara Arango Rodriguez

Dedicatoria

A mi familia, por creer en mi capacidad y apoyarme en todo momento a lo largo de mi vida, por estar siempre conmigo y darme la motivación que a veces me hace falta.

Agradecimiento

A quienes me brindaron la oportunidad de poder realizar este trabajo y a mis amigos que me de alguna manera apoyaron en realizarlo.

Resumen

El objetivo del presente informe es dar a conocer las actividades realizadas en la Unidad Ejecutora 003, como asistente en el área de informática, donde apliqué conocimientos teóricos y prácticos adquiridos durante los años de estudio en la Universidad Nacional de Moquegua, realizando diversas labores como realizar mantenimiento y reparación a los equipos de cómputo, instalación y configuración de software y hardware, instalación y configuración de redes de computadoras, soporte técnico, etc.

Durante el periodo laborado en la entidad, aprendí muchas cosas que complementaron la formación que tuve, especialmente al realizar una auditoría a la entidad, utilizando la ISO/IEC 17799, con la cual tuve la oportunidad de entender con mayor claridad la importancia de aplicar ciertos estándares y normas en cualquier institución o empresa.

Las conclusiones se muestran más adelante, así como también la información recabada de la entidad, junto con fotos de referencia de acuerdo a los criterios evaluados.

Abstract

The objective of this report is to publicize the activities carried out in the Executing Unit 003, as an assistant in the computer area, where I applied theoretical and practical knowledge acquired during the years of study at the National University of Moquegua, performing various tasks such as maintenance and repair of computer equipment, installation and configuration of software and hardware, installation and configuration of computer networks, technical support, etc.

During the period I worked in the entity, I learned many things that complemented the training I had, especially when auditing the entity, using ISO/IEC 17799, with which I had the opportunity to understand more clearly the importance of applying certain standards and norms in any institution or company.

The conclusions are shown below, as well as the information collected from the entity, along with reference photos according to the criteria evaluated.

Índice General

Dedicatoria II

Agradecimiento III

Resumen IV

Abstract V

Índice General VI

Índice de Imágenes VIII

Índice de Tablas XI

Acrónimos y Abreviaturas XII

Introducción 1

Capítulo I Aspectos Generales 2

1.1. Descripción de la Empresa /Institución (donde labora o laboró) 2

1.1.1 Ubicación 2

1.1.2 Accesibilidad 2

1.1.3 Visión y misión de la empresa 2

1.1.4 Historia 3

Capitulo II Descripción de una actividad específica 3

2.1. Actividades realizadas: 4

2.1.1. Logros alcanzados: 4

2.1.2. Deficiencias encontradas: 4

2.2. Implementación De La NTP/ISO 17799 5

2.2.1 Objetivo 5

2.2.2. Objetivos Específicos..... 5

2.2.3. Documentos..... 5

2.2.4. Criterios De Evaluación..... 6

Capitulo III Antecedentes Y Objetivos..... 23

3.1. Antecedentes Internacionales..... 23

3.2. Antecedentes Nacionales..... 23

3.3. Objetivos..... 24

3.3.1. Objetivo General..... 24

3.3.2. Objetivos específicos..... 25

Capitulo IV Discusiones o Aportes..... 26

Conclusiones y recomendaciones..... 26

Conclusiones..... 26

Recomendaciones..... 26

Bibliografía..... 28

Índice de Imágenes

Figura 1 Ubicación De La UE 003 2

Figura 2 Control de asistencia por huella digital. 9

Figura 3 Señalización de aforo, no fumar y extintor. 10

Figura 4 Personal De Seguridad. 11

Figura 5 Archivo Central. 11

Figura 6 Señalizaciones. 12

Figura 7 Cuaderno de concurrencias. 12

Figura 8 Instalaciones de ductos y cables 13

Figura 9 Aglomeración en oficina de infraestructura. 13

Figura 10 Cables Amontonados, Oficina De Informática Y Oficina Infraestructura. 14

Figura 11 Instalación de cables de corriente se cruzan con la instalación de cables de red. . 14

Figura 12 Luces de emergencia desconectadas. 15

Figura 13 Servidores en el área de informática. 16

Figura 14 Acondicionador de aire no instalado. 17

Figura 15 Hoja de evaluación de las Políticas de seguridad 30

Figura 16 Hoja de evaluación: Aspectos organizativos para la seguridad 1. 31

Figura 17 Hoja De Evaluación: Aspectos Organizativos Para La Seguridad 2. 32

Figura 18 Hoja De Evaluación: Aspectos Organizativos Para La Seguridad 3 33

Figura 19 Hoja de Evaluación: Clasificación y control de activos 34

Figura 20 Hoja de evaluación: Seguridad en recursos humanos 1 35

Figura 21 Hoja de evaluación: Seguridad en recursos humanos 2 36

Figura 22 Hoja de evaluación: Seguridad física y del entorno 1 37

Figura 23 Hoja de evaluación: Seguridad física y del entorno 2 38

Figura 24 Hoja de evaluación: Seguridad física y del entorno 3 39

Figura 25 Hoja de evaluación: Seguridad física y del entorno 4 40

Figura 26 Hoja de evaluación: Seguridad física y del entorno 5 41

Figura 27 Hoja de evaluación: Seguridad física y del entorno 6 42

Figura 28 Hoja de evaluación: Seguridad física y del entorno 7 43

Figura 29 Hoja de evaluación: Gestión de Comunicaciones y operaciones 1..... 44

Figura 30 Hoja de evaluación: Gestión de Comunicaciones y operaciones 2..... 45

Figura 31 Hoja de evaluación: Gestión de Comunicaciones y operaciones 3..... 46

Figura 32 Hoja de evaluación: Gestión de Comunicaciones y operaciones 4..... 47

Figura 33 Hoja de evaluación: Gestión de Comunicaciones y operaciones 5..... 48

Figura 34 Hoja de evaluación: Gestión de Comunicaciones y operaciones 6..... 49

Figura 35 Hoja de evaluación: Gestión de Comunicaciones y operaciones 7..... 50

Figura 36 Hoja de evaluación: Gestión de Comunicaciones y operaciones 8..... 51

Figura 37 Hoja de evaluación: Gestión de Comunicaciones y operaciones 9..... 52

Figura 38 Hoja de evaluación: Gestión de Comunicaciones y operaciones 10..... 53

Figura 39 Hoja de evaluación: Control de Acceso 1..... 54

Figura 40 Hoja de evaluación: Control de Acceso 2..... 55

Figura 41 Hoja de evaluación: Control de Acceso 3..... 56

Figura 42 Hoja de evaluación: Control de Acceso 4..... 57

Figura 43 Hoja de evaluación: Control de Acceso 5..... 58

Figura 44 Hoja de evaluación: Control de Acceso 6..... 59

Figura 45 Hoja de evaluación: Adquisición, desarrollo y mantenimiento de sistemas 1 60

Figura 46 Hoja de evaluación: Adquisición, desarrollo y mantenimiento de sistemas 2 61

Figura 47 Hoja de evaluación: Adquisición, desarrollo y mantenimiento de sistemas 3 62

Figura 48 Hoja de evaluación: Adquisición, desarrollo y mantenimiento de sistemas 4 63

Figura 49 Hoja de evaluación: Adquisición, desarrollo y mantenimiento de sistemas 5 64

Figura 50 Hoja de evaluación: Gestión de incidentes en la seguridad de la información 1 ... 67

Figura 51 Hoja de evaluación: Gestión de incidentes en la seguridad de la información 2 ... 68

Figura 52 Hoja de evaluación: Cumplimiento 1 ... 69

Figura 53 Hoja de evaluación: Cumplimiento 2 ... 70

Figura 54 Hoja de evaluación: Cumplimiento 3 ... 71

Figura 55 Hoja de evaluación: Cumplimiento 4 ... 72

Figura 56 Cierre de Auditoría ... 73

Figura 57 Cierre de Auditoría 2 ... 74

Índice de Tablas

Tabla 1 Cuadro de requerimientos funcionales SIAF 65

Acrónimos y Abreviaturas

NTP : Normas técnicas peruanas.

ISO : (Internacional Organization for Standardization) es la Organización Internacional de Normalización.

UE : Unidad Ejecutora

ANSI : El American National Standards Institute (Instituto Nacional Estadounidense de Estándares)

EIA : Asociación de Industrias Electrónicas

TIA : Asociación de la Industria de las Telecomunicaciones

PCM : Presidencia del Consejo de Ministros

SIAF : Sistema Integrado de Administración Financiera

ERP : Enterprise Resource Planning, que significa “sistema de planificación de recursos empresariales”

PYMES : La pequeña y mediana empresa

Introducción

El presente informe muestra una descripción de las actividades desarrolladas en la Unidad Ejecutora Subregión de Desarrollo Ilo 003, que se encuentra ubicada en la Avenida Venecia Nro. 222 Ilo– Perú.

Las actividades que se realizaron en la Oficina de Informática consistieron en Mantenimiento y Reparación de los equipos de cómputo (PCS), Instalación y Configuración de Software a las PCS, Instalación y configuración de Redes de computadoras, Soporte técnico, así como la realización de una auditoria interna utilizando la NTP/ISO 17799, código de buenas prácticas para la gestión de la seguridad de la información.

El informe contiene el desarrollo íntegro y descriptivo de las funciones realizadas en la Unidad Ejecutora Subregión de Desarrollo Ilo, enfocándose en los resultados obtenidos al realizar la auditoria interna aplicando la NTP/ISO 17799, la cual fue de gran valor para reconocer la importancia de aplicar estándares y normas en las instituciones o empresas, mejorando así la seguridad de la información.

Capítulo I

Aspectos Generales

1.1. Descripción de la Empresa /Institución (donde labora o laboró)

1.1.1 Ubicación

Departamento : Moquegua

Provincia : Ilo

Distrito : Ilo

Dirección : Av. Venecia Nro. 222

1.1.2 Accesibilidad

Figura 1

Ubicación De La UE 003



Nota. Ubicación extraída de Google maps.

1.1.3 Visión y misión de la empresa

Visión

Somos una institución moderna, integrada que brinda servicios de calidad y eficiencia con capacidad de generar políticas de desarrollo sostenibles y definidas sobre la base de su personal con vocación de servicio, generando un impacto positivo en bienestar de la población moqueguana, con una adecuada priorización y enfoque de la inversión pública.

Misión

Conducir la gestión pública regional de acuerdo a sus competencias exclusivas, compartidas y delegadas por la ley orgánica de su creación en el marco de las políticas nacionales y sectoriales para contribuir al desarrollo integral y sostenible de la región.

1.1.4 Historia

UNIDAD EJECUTORA SUB REGION DE DESARROLLO ILO 003 especializada en ACTIVIDADES DE LA ADMINISTRACIÓN PÚBLICA EN GENERAL. Fue creada y fundada el 18/01/2010, registrada dentro de las sociedades mercantiles y comerciales como una GOBIERNO REGIONAL, LOCAL.

La Gerencia Sub Regional de Ilo como parte integrante del GOBIERNO REGIONAL DE MOQUEGUA, es la encargada de formular, programar coordinar, ejecutar las acciones de desarrollo en la provincia de Ilo; depende jerárquica y administrativamente de la Gerencia General Regional.

Capitulo II

Descripción de una actividad específica

2.1. Actividades realizadas:

- Mantenimiento y reparación de los equipos de cómputo (pcs).
- Instalación y configuración de software a las pcs.
- Soporte técnico: En caso de virus, fallas en otro hardware, recurso de emergencias, fallas de la impresora.
- Instalación y configuración de la red: Cableado estructurado, configuración de la red de internet, crear grupo de trabajo, compartir impresora, compartir unidades de red.

2.1.1. Logros alcanzados:

- Buen resultado en el proceso del diagnóstico de pc's.
- Brindar un mejor servicio en mantenimiento y reparación de pc's, con la finalidad de que los usuarios no pierdan mucho tiempo en para la realización de sus labores.
- Conocimiento de la estructura básica de una pc.
- Experiencia en el mantenimiento de las pc's.
- Conocimiento en la instalación de recursos del propio sistema operativo y diversos programas.
- Mejora en el desenvolvimiento con personas en este caso con los demás trabajadores, usuarios de las pc's, siguiendo un plan integral de operatividad acorde con las exigencias de la institución.
- Mayor dominio en el manejo de aplicativos en documentos (el paquete de microsoft office), hojas de cálculo y soluciones inmediatas.
- Conocimiento en instalación y configuración de redes de computadoras.
- Conocimiento en configuración de puntos de acceso y repetidores de red.
- Responsabilidad, seriedad y puntualidad en el centro de trabajo.

2.1.2. Deficiencias encontradas:

- Falta de antivirus actualizados y activados.

- Cables de red sueltos, rotos y canaletas mal ubicadas.
- Deficiencias de algunos equipos por la antigüedad.
- Falta de un control de ingreso y salida de equipos y materiales en el área de computación e informática.

2.2. Implementación De La NTP/ISO 17799

2.2.1 Objetivo

El objetivo de la auditoría interna realizada es revisar y evaluar los controles, sistemas, procedimientos de informática, los equipos de cómputo (su instalación, utilización, eficiencia y seguridad) y distintos aspectos más que participan en el procesamiento de la información, tomando en cuenta distintas normas y leyes para realizar las recomendaciones necesarias y que así se logre obtener un mejor y seguro ambiente laboral y una utilización más eficiente y segura de la información.

2.2.2. Objetivos Específicos

- Evaluar los procedimientos de control de operación, analizar su estandarización y evaluar el cumplimiento de los mismos.
- Evaluar la forma como se administran los dispositivos de almacenamiento básico.
- Evaluar el control que se tiene sobre el mantenimiento y las fallas de las Pcs.
- Verificar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro del área de informática.

2.2.3. Documentos

- Políticas, estándares, normas y procedimientos.
- Planes de seguridad y continuidad
- Organigrama y manual de funciones.
- Registros
- Entrevistas
- Requerimientos de Usuarios

2.2.4. Criterios De Evaluación

2.2.4.1. Política De Seguridad (Anexo 01).

Evidencias Positivas.

- Si bien es cierto que la Unidad Ejecutora Subregión de Desarrollo Ilo 003 no cuenta con un Plan de Seguridad, existe una política de seguridad hablada, la cual es respetada y acatada por el personal.
- Las responsabilidades generales y específicas en cuanto al cuidado de la información están definidas a pesar de que no se cuente con la documentación.

Evidencias Negativas.

- No cuenta con un Plan de Seguridad aprobado y publicado. (HALLAZGO)
- No hay un calendario establecido de revisión de la las políticas de seguridad para su implementación.

Conclusiones.

No contar con un Plan de seguridad ni un Plan Estratégico de Tecnologías de Información lleva consigo muchos riesgos para la institución ya que las personas que laboral allí pueden apropiarse, dañar o modificar la información.

Recomendaciones.

- Elaboración del Plan de Seguridad y el Plan Estratégico de Tecnologías de Información. Tener en cuenta principios establecidos en el Art. Nº 23 de la Ley de seguridad y salud en el trabajo Nº 29783.
- Elaborar un calendario para la revisión de las políticas de seguridad.

2.2.4.2. Aspectos Organizativos Para La Seguridad (Anexo 02).

Evidencias Positivas.

- En la organización interna existen responsables sobre la seguridad de activos lógicos y físicos.

Evidencias Negativas.

- No existe un comité multidisciplinario que apoye activamente al control de la seguridad de la información de la organización.
- Existen computadores que no son compatibles con el software requerido. (HALLAZGO)
- Algunos computadores son demasiado antiguos y presentan fallas. (HALLAZGO)

Conclusiones.

El contar con especificaciones distintas, para los ordenadores, según las necesidades del área es adecuado, mas no se debe descuidar el mantenimiento ni reemplazo de los equipos.

Recomendaciones.

- Conformar un comité multidisciplinario que apoye al control de la seguridad.
- Reemplazar computadores antiguos (Art. 22º TUO Inc. b) Reglamento de la Ley del Impuesto a la Renta) y realizar un mantenimiento periódicamente.
- Optar por equipos de cómputo compatibles con el software a utilizar. Ley 28612 Ley que norma el Uso, Adquisición y Adecuación del software.

2.2.4.3. Clasificación Y Control De Activos (Anexo 03).

Evidencias Positivas.

- Los activos físicos y lógicos de la Unidad Ejecutora Subregión de Desarrollo Ilo 003, se encuentran debidamente inventariados
- Se han asignado responsabilidades de propiedad de activos, tanto físicos como lógicos y toda la información asociada por parte de la organización.
- Se ha clasificado la información de los activos en grados de prioridades y protección en función de su valor, requisitos legales, sensibilidad y criticidad para la organización.
- Se ha restringido el uso de internet, sólo para fines laborales y no para uso de redes sociales, a no ser que sea necesario para algunas labores.

Evidencias Negativas.

- Algunos equipos o accesorios informáticos son prestados entre oficinas sin un documento de por medio. (HALLAZGO)
- Cuando un equipo pasa a soporte técnico, no se emite un informe o documento, a no ser que el equipo ya no funcione y deba ser internado en almacén. (HALLAZGO)
- Los empleados no respetan las reglas respecto al uso de internet sólo para fines laborales.

Conclusiones.

Es necesario el inventario de activos y asignar responsabilidades de propiedad. Así se asegura la integridad de los activos y el correcto funcionamiento de la institución, ya que el activo más importante es la información.

Recomendaciones.

- Documentar los préstamos de accesorios de oficina, así como el equipo de cómputo que es enviado a soporte técnico. (Ley Nº 29151, Ley General del Sistema Nacional de Bienes Estatales)
- Revisar que los computadores no cuenten con software que inhabilite las restricciones de acceso a internet. (Reglamento interno)

2.2.4.4. Seguridad En Recursos Humanos (Anexo 04).

Evidencias Positivas.

- Las funciones y responsabilidades de los empleados han sido designadas de acuerdo al Manual De Organización Y Funciones de la Gerencia Sub Regional de Ilo.
- Para el contrato de Personal se crean perfiles según las necesidades de la Unidad Ejecutora o del área en cuestión.

- Al momento de que un empleado concluye su trabajo se le retira todos los activos que se le entregaron.
- Cuentan con plan de evacuación
- Cuentan con sistema de control de asistencia por huella digital para trabajadores nombrados.

Figura 2

Control de asistencia por huella digital.



Evidencias Negativas.

- No existe un proceso formal disciplinario para empleados que cometan una apretura en la seguridad de la información.
- Existe un continuo intercambio de personal entre las áreas, lo cual, algunas veces, genera retraso en actividades.
- El plan de evacuación no ha sido comunicado ni publicado. (HALLAZGO)

Conclusiones.

Es importante que exista un control adecuado de la seguridad en recursos humanos en la Unidad Ejecutora, antes, durante y después del empleo.

Recomendaciones.

- Comunicar a todo el personal el plan de evacuación en caso de desastres, y pegar un mapa de evacuación en los pasillos de la institución. (Ley 29783, ley de seguridad y salud en el trabajo)
- Implementar un proceso disciplinario para los empleados que cometan una apertura en la seguridad de la información.

2.2.4.5. Seguridad Física Y Del Entorno (Anexo 05).

Evidencias Positivas.

- Existen señalizaciones y personal de seguridad para evitar el acceso de personas no autorizadas a áreas restringidas.

Figura 3

Señalización de aforo, no fumar y extintor.



- Hay personal de seguridad.

Figura 4

Personal De Seguridad.



- La información sensible, de años anteriores, es almacenada en el área de Archivo Central, los archivos y documentos del año en curso son almacenados en las oficinas donde se originan o recepcionan, hasta que pasen al Archivo Central. Cuentan con controles de seguridad.

Figura 5

Archivo Central.



- Cuentan con equipos de extinción, y señalización.

Figura 6

Señalizaciones.



- Los equipos cuentan con claves de usuario para su uso.
- Cuentan con un cuaderno de concurrencias

Figura 7

Cuaderno de concurrencias.



Evidencias Negativas.

- La seguridad de instalaciones, ductos y cables es regular. (HALLAZGO)

Figura 8

Instalaciones de ductos y cables



- En cuanto a seguridad física, algunas oficinas albergan muchos muebles y equipos, cuyas conexiones de corriente y red, en su mayoría, no son adecuadas, hay cables sobresalientes, amontonados. (HALLAZGO)

Figura 9

Aglomeración en oficina de infraestructura.



Figura 10

Cables Amontonados, Oficina De Informática Y Oficina Infraestructura.

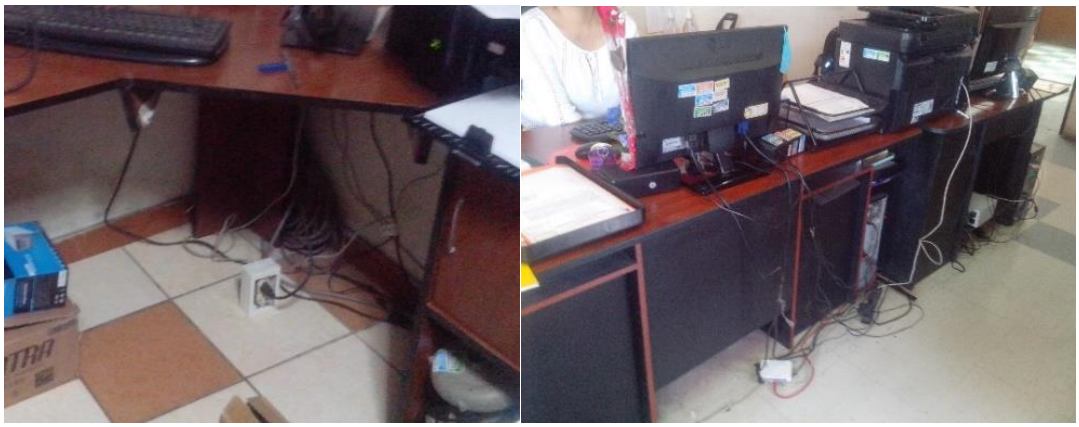


Figura 11

Instalación de cables de corriente se cruzan con la instalación de cables de red.



- No se registran a los visitantes, sólo se pide DNI cuando no son conocidos.
- Cuentan con luces de emergencia pero no están en funcionamiento. (HALLAZGO)

Figura 12

Luces de emergencia desconectadas.



- No cuentan con alarma contra incendios. (HALLAZGO)
- No existe una política formal que limite el uso de equipos de fotografía, video, audio.

Conclusiones.

Existen muchas deficiencias en cuanto a la seguridad física que deben ser absueltas, no sólo es importante asignar responsabilidad, también lo es contar con un buen ambiente de trabajo, donde no existan riesgos para el empleado.

Recomendaciones.

- Reemplazar el cableado de red deteriorado e instalarlo correctamente. ANSI/EIA/TIA 569 Normas cómo enrutar el cableado. TIA/EIA 606-A Lineamientos administración de cableado.
- Tener luces de emergencia operativas. (Norma A.130 Requisitos de seguridad Art.40°)
- Implantar plan de contingencia y alarma de incendios. (D.S. Nº 066-2007-PCM APROBACIÓN REGLAMENTO DE INSPECCIONES TÉCNICAS DE SEGURIDAD EN DEFENSA CIVIL Art.10°)
- Controlar el acceso de los visitantes.
- Instalar el aire acondicionado y mejorar el área de los servidores, así como su instalación.

2.2.4.6. Gestión De Comunicaciones Y Operaciones (Anexo 06).

Evidencias Positivas.

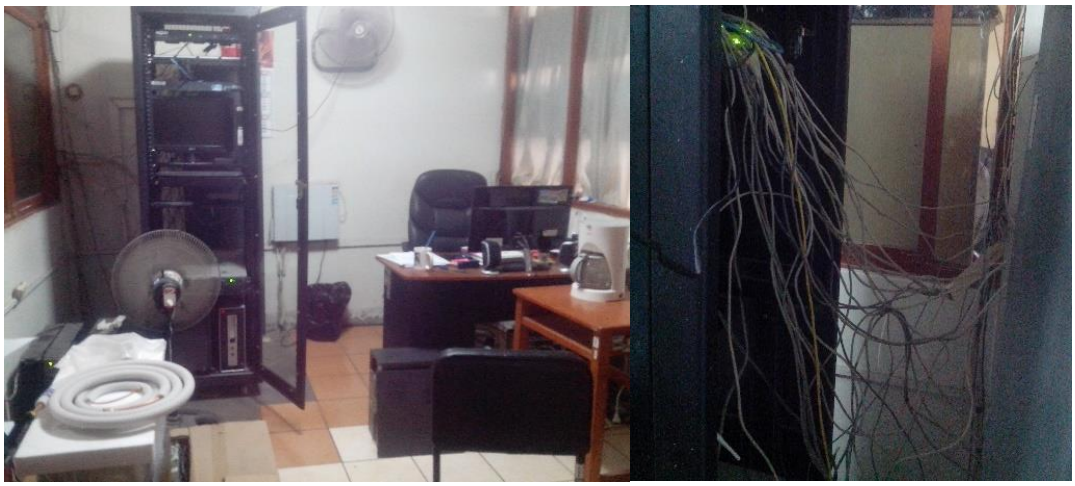
- Se cuenta con un manual de procedimiento para la realización de los backup y el manteamiento de equipos.
- Cuando un equipo deja de funcionar, la información que contenga es borrada y luego el equipo es almacenado.
- No está permitido que los empleados traigan sus equipos o accedan a redes sociales.
- Cuentan con antivirus.
- Existen responsabilidades y procedimientos para la gestión de equipos remotos.
- Hay seguridad en la mensajería electrónica.

Evidencias Negativas.

- No hay una correcta instalación de los servidores. (HALLAZGO)

Figura 13

Servidores en el área de informática.



- El aire acondicionado de lo que se supone es el área de servidores no está instalado.

Figura 14

Acondicionador de aire no instalado.



- No existen instrucciones para manejar errores u otras condiciones excepcionales que puedan ocurrir durante la tarea de ejecución.
- No se hacen revisiones regulares del software y los datos contenidos en los sistemas que soportan procesos críticos de la institución.

Conclusiones.

Restringir el acceso a redes sociales a los empleados colabora a que éstos se centren en sus responsabilidades y realicen un mejor trabajo sin distracciones.

Enfocarse en la seguridad de las comunicaciones y operaciones es importante para mejorar el cumplimiento de los objetivos de la institución.

Recomendaciones.

- Acondicionar la sala de servidores (ANSI/TIA/EIA-569) y mejorar la instalación del cableado, utilizar etiquetas para identificar las rutas de los cables. TIA/EIA – 606.

- Implementar controles apropiados para evitar riesgos (sistemas de cifrado, copias de seguridad, sistemas de detección de intrusos, actualizaciones de software, antivirus o cortafuegos).
- Hacer revisiones regulares del software y los datos contenidos.
- Implementar planes de seguridad.

2.2.4.7. Control De Acceso (Anexo 07)

Evidencias Positivas.

- En cuanto a los Sistemas de información que usan, cuenta con perfiles de acceso autorizados también cada usuario cuenta con un identificador distinto.
- Cuando un empleado cambia de área o deja de laboral en la Unidad Ejecutora, se bloquea su cuenta.
- Los usuarios de SIAF cuentan con diferentes privilegios según el área donde se trabaje por ser un sistema ERP.
- Los empleados, en su mayoría, cuentan con buenas prácticas al momento de usar los equipos o al no usarlos ellos lo apagan y lo desconectan.

Evidencias Negativas.

- No existe un proceso de revisión periódica de los derechos de acceso de los usuarios.
- No todos los usuarios siguen buenas prácticas de seguridad para la selección de contraseñas.
- No todos los usuarios tienen buenas prácticas con los equipos desatendidos.
- No existen mensajes de ayuda, sino de error, que guíen durante el proceso de conexión de usuarios no autorizados.
- No hay un registro de contraseñas anteriormente utilizadas.
- No existe una política formal con medidas de seguridad al usar dispositivos informáticos.
- No existe seguridad física real en cuanto al uso de móviles para el trabajo.

Conclusiones.

Los responsables de cada área, así como los empleados en general, que tengan acceso a los sistemas utilizados deben contar con un usuario y contraseña propia, ya que deben existir niveles de autenticación.

Recomendaciones.

- Realizar una revisión periódica de los derechos de acceso de los usuarios.
- Concientizar a los empleados con las buenas prácticas para los equipos desatendidos.
- Revisar periódicamente los derechos de acceso de los usuarios.
- Implementar políticas de seguridad de protección contra riesgos al usar equipos informáticos.

2.2.4.8. Adquisición, Desarrollo Y Mantenimiento De Sistemas (Anexo 08 y 09).

Evidencias Positivas.

- Sólo el área de informática puede realizar la adquisición de algún software.
- Se realiza un análisis de los requisitos de seguridad de los sistemas o software a adquirir.
- Existe validación de los datos de entrada y salida.
- Se utilizan medidas criptográficas.
- Sólo el administrador capacitado realiza actualización de las librerías de los programas.

Evidencias Negativas.

- No existe una política basada en la evaluación de riesgos.
- No hay supervisión de almacenamiento de datos en dispositivos removibles.
- No todos los datos almacenados son encriptados.
- Se utiliza software sin licencia, crackeado y no software libre. (HALLAZGO)

Conclusiones

Descuidar la seguridad en cuanto a la adquisición y desarrollo de software puede traer graves consecuencias para la institución.

Recomendaciones.

- Asegurar que el software utilizado sea legal y se utilice en cumplimiento de los términos de la licencia. R.M. N° 073-2004-PCM.
- Implementar políticas para la evaluación de riesgos.
- Encriptar los datos almacenados en dispositivos removibles.

2.2.4.9. Gestión De Incidentes (Anexo 10).

Evidencias Positivas.

- Existen formularios de reporte de eventos en la seguridad de información.
- Existen acciones para recuperación de aperturas de seguridad y control de fallas del sistema.
- El personal ha sido informado sobre la seguridad de la información.

Evidencias Negativas.

- No hay registro de auditorías informáticas internas ni externas.
- No se documentan los incidentes de seguridad de información. (HALLAZGO)

Conclusiones.

Gestionar adecuadamente los incidentes en la seguridad de la información y concientizando al personal en cuanto a ello, ayudará a reducir dichos incidentes.

Recomendaciones.

- Monitorear actividades y generar reportes permanentemente.
- Realizar procesos de concienciación sobre la seguridad de la información.
- Documentar registros de incidentes de seguridad para los procesos de retroalimentación. NTP-ISO/IEC 17799

- Implementar un proceso para el tratamiento y custodia de evidencia ante un incidente de seguridad.

2.2.4.10. Gestión De Continuidad Del Negocio.

Evidencias.

Debido a que no se trata de un negocio, la Unidad Ejecutora no cuenta con planes para la continuidad del negocio. Sin embargo, la presidencia del consejo de ministros aprobó lineamientos para la Continuidad Operativa de las entidades públicas;

Conclusiones.

Este control no aplica para el alcance de este trabajo, ya que se trata de una institución gubernamental y no de un negocio.

Recomendaciones.

Establecer normas de seguridad de acuerdo con los lineamientos para la Continuidad Operativa.

2.2.4.11. CUMPLIMIENTO (anexo 11).

Evidencias Positivas.

- Los activos están registrados apropiadamente.
- Tienen un cuaderno de ocurrencias, donde se anotan sucesos como accidentes, robos, etc.
- Se adoptan acciones disciplinarias y/o legales apropiadas, cuando se identifica el uso de recursos para fines no autorizados.

Evidencias Negativas.

- No se cuenta con un reglamento disciplinario para empleados.

- No existe un uso de herramientas adecuadas de auditoria.
- Hay software instalado no autorizado y sin licencia.(HALLAZGO)

Capitulo III

Antecedentes Y Objetivos

3.1. Antecedentes Internacionales

(Gómez Arcila & Moncayo Viveros, 2006) Sistema De Gestión De Incidentes De Seguridad Basado En Norma ISO 17799:2005 Aplicado A Pequeñas Y Medianas Empresas En Colombia, Orientado A Sistemas Operativos Linux Y Windows. Universidad EIA.

Donde primero plantean evaluar la aplicabilidad de las mejores prácticas en gestión de incidentes de seguridad con base en la norma ISO 17799:2005 y la normatividad legal colombiana existente. Lo que les permite analizar el impacto de la combinación de estos aspectos al sector de la industria para el correcto y eficiente manejo de incidentes de seguridad. Seguidamente plantea investigar en el marco de las pequeñas y medianas empresas en Colombia, la aplicación de los ítems mencionados anteriormente, y tendencias en términos de monitoreo y seguimiento de incidentes de seguridad basándonos en las normas y propuestas realizadas por empresas exitosas e instituciones con experiencia. Luego de haber tenido la oportunidad de realizar un estudio adecuado, se espera localizar con mayor facilidad, las inconsistencias, riesgos y puntos de mejoramiento en la gestión de incidentes de seguridad en los ambientes operativos Linux y Windows para las PYMES.

(Soriano Rodríguez, 2007) Implementación de seguridades de red en el centro de cómputo de la Facultad de Ingeniería Industrial de la Universidad de Guayaquil, basado en el estándar internacional ISO 17799. Con lo que busca proveer de un código de buenas prácticas para realizar la Gestión de la Seguridad de Red en el Centro de Cómputo de la Facultad de Ingeniería Industrial, el cual puede ser tomado marco de referencia durante el proceso de determinación y definición de políticas de seguridad.

3.2. Antecedentes Nacionales

(Calisaya Sana & Tarrillo Villegas, 2018), En su trabajo de tesis denominado: “Implementación de controles de seguridad para la protección de datos personales en una Universidad Privada para el

cumplimiento parcial de la Ley 29733 basado en los controles de seguridad de la NTP-ISO/IEC 17799:2007." se enfocó en "Medidas de Seguridad" del Reglamento de la LPDP en las áreas de Dirección General de Tecnología de Información (DIGETI) y Secretaría General (SG) de la Universidad Peruana Unión, por lo tanto, se implementó controles de seguridad basados en la NTP-ISO/IEC 17799:2007, para promover una cultura de seguridad de la información e impulsar el cumplimiento de la LPDP a nivel corporativo.

(Fernández Fernández, 2015), Modelo de gestión de riesgos de TI de acuerdo con las exigencias de la SBS, basados en las ISO/IEC 27001, ISO/IEC 17799, Magerit para la Caja de Ahorro y Créditos SIPAN SA. Con esta investigación se demostró que con un modelo de gestión de riesgos implementado, tomando como referencia a los estándares ISO/IEC 27001, ISO 17799 y la metodología MagerIT, se puede lograr mayor efectividad en el cálculo de los niveles de riesgos de los diferentes activos de TI en la etapa de evaluación de los riesgos; así como también en el tratamiento de éstos, a través de la implantación y seguimiento de los controles, siempre en concordancia y en cumplimiento con los requerimientos mínimos de la SBS para estos fines. Para ello se tomó como caso experimental, la CRAC Sipán SAC.

(Villena Acuña , 2015), Aplicación De La Norma Técnica Peruana ISO 17799 Al Desarrollo Del Sistema De Información De Gestión Administrativa Siga Modulo Logístico En La Dirección Subregional De Salud Alto Huallaga Unidad Ejecuta 403 Tocache. En donde plantea la aplicación de la norma técnica peruana ISO 17799 al desarrollo del sistema de información de gestión administrativa, esperando binde beneficios que permitan tener un plan de contingencia de todo lo relacionado a la seguridad de la información.

3.3. Objetivos

3.3.1. Objetivo General.

El objetivo de la auditoría interna realizada es revisar y evaluar los controles, sistemas, procedimientos de informática, los equipos de cómputo (su instalación, utilización, eficiencia y

seguridad) y distintos aspectos más que participan en el procesamiento de la información, tomando en cuenta distintas normas y leyes para realizar las recomendaciones necesarias y que así se logre obtener un mejor y seguro ambiente laboral y una utilización más eficiente y segura de la información.

3.3.2. Objetivos específicos.

Evaluar los procedimientos de control de operación, analizar su estandarización y evaluar el cumplimiento de los mismos.

Evaluar la forma como se administran los dispositivos de almacenamiento básico.

Evaluar el control que se tiene sobre el mantenimiento y las fallas de las Pcs.

Verificar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro del área de informática.

Capitulo IV

Discusiones o Aportes

Es de suma importancia no solo realizar un mantenimiento periódico de los equipos de cómputo, sino supervisar que se esté cumpliendo con las labores y procedimientos señalados por las políticas de la institución; pero sobretodo aplicar normas existentes como las NTP/ISO para mejorar la calidad de la seguridad de la información, entre otros. Así también estar al pendiente de las ocurrencias, para poder realizar una retroalimentación y mejorar la forma en que se realizan las labores.

Conclusiones y recomendaciones

Conclusiones

Con el manteniendo brindado a los equipos de cómputo, se logró resolver los problemas acarreados por la falta de este, haciendo más eficiente el funcionamiento de dichos equipos y el rendimiento del personal que lo emplea.

Con la auditoría se dieron recomendaciones que se han ido tomando en cuenta poco a poco, como el cambio del cableado de red deteriorado y la instalación de un repetidor de red, lo que resolvió problemas de conectividad en algunas áreas.

Recomendaciones

Implementar un reglamento disciplinario para los empleados cuando se identifique el uso de recursos para fines no autorizados.

Instruir al personal, responsable de los sistemas de información, en el uso de herramientas adecuadas de auditoría.

Documentar registros de incidentes de seguridad para los procesos de retroalimentación. NTP-ISO/IEC 17799.

Implementar un proceso para el tratamiento y custodia de evidencia ante un incidente de seguridad.

Comprar licencias de software, u optar por utilizar software gratuito. R.M. N° 073-2004-PCM.

Bibliografía

Calisaya Sana, C. Y., & Tarrillo Villegas, M. (2018). *Implementación de controles de seguridad para la protección de datos personales en una Universidad Privada para el cumplimiento parcial de la Ley 29733 basado en los controles de seguridad de la NTP-ISO/IEC 17799:2007.* http://hdl.handle.net/20.500.12840/1380

Fernández Fernández, D. (2015). *Modelo de gestión de riesgos de TI de acuerdo con las exigencias de la SBS, basados en las ISO/IEC 27001, ISO/IEC 17799, Magerit para la Caja de Ahorro y Créditos SIPAN SA.* UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO, Chiclayo. http://hdl.handle.net/20.500.12423/540

Gómez Arcila, C., & Moncayo Viveros, S. (2006). *Sistema De Gestión De Incidentes De Seguridad Basado En Norma Iso 17799:2005 Aplicado A Pequeñas Y Medianas Empresas En Colombia, Orientado A Sistemas Operativos Linux Y Windows.* Trabajo de grado, Medellín. https://repository.eia.edu.co/handle/11190/4440

Soriano Rodríguez, F. J. (2007). *Implementación de seguridades de red en el centro de cómputo de la Facultad de Ingeniería Industrial de la Universidad de Guayaquil, basado en el estándar internacional ISO 17799.* Tesis de grado, Universidad de Guayaquil, Guayaquil. http://repositorio.ug.edu.ec/handle/redug/56612

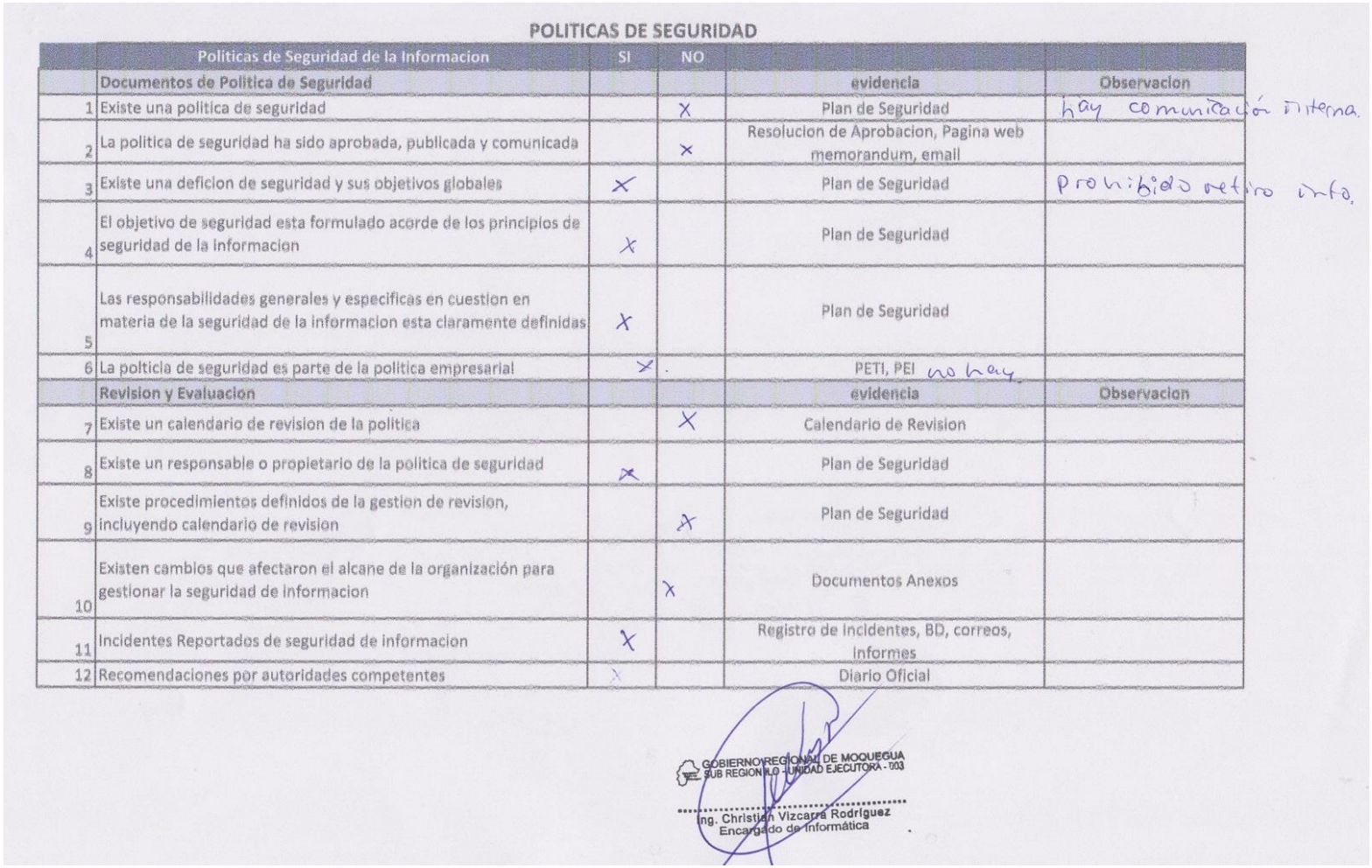
Villena Acuña , J. L. (2015). *Aplicación De La Norma Técnica Peruana ISO 17799 Al Desarrollo Del Sistema De Información De Gestión Administrativa Siga Modulo Logístico En La Dirección Subregional De Salud Alto Huallaga Unidad Ejecuta 403 Tocache.* Universidad Nacional Agraria De La Selva, Tingo María. http://repositorio.unas.edu.pe/handle/UNAS/1035

ANEXOS

Anexo 01

Figura 15

Hoja de evaluación de las Políticas de seguridad



POLITICAS DE SEGURIDAD

	Politicas de Seguridad de la Informacion	SI	NO		
	Documentos de Politica de Seguridad			**evidencia**	**Observacion**
1	Existe una politica de seguridad		X	Plan de Seguridad	hay comunicación interna.
2	La politica de seguridad ha sido aprobada, publicada y comunicada		X	Resolucion de Aprobacion, Pagina web memorandum, email	
3	Existe una deficion de seguridad y sus objetivos globales	X		Plan de Seguridad	Prohibido retiro info.
4	El objetivo de seguridad esta formulado acorde de los principios de seguridad de la informacion	X		Plan de Seguridad	
5	Las responsabilidades generales y especificas en cuestion en materia de la seguridad de la informacion esta claramente definidas	X		Plan de Seguridad	
6	La politicia de seguridad es parte de la politica empresarial	X		PETI, PEI no hay.	
	Revision y Evaluacion			**evidencia**	**Observacion**
7	Existe un calendario de revision de la politica		X	Calendario de Revision	
8	Existe un responsable o propietario de la politica de seguridad	X		Plan de Seguridad	
9	Existe procedimientos definidos de la gestion de revision, incluyendo calendario de revision		X	Plan de Seguridad	
10	Existen cambios que afectaron el alcane de la organización para gestionar la seguridad de informacion		X	Documentos Anexos	
11	Incidentes Reportados de seguridad de informacion	X		Registro de incidentes, BD, correos, informes	
12	Recomendaciones por autoridades competentes	X		Diario Oficial	

GOBIERNO REGIONAL DE MOQUEGUA
SUB REGION ILO - UNIDAD EJECUTORA - 003

Ing. Christian Vizcarra Rodriguez
Encargado de Informática

Anexo 02

Figura 16

Hoja de evaluación: Aspectos organizativos para la seguridad 1.

ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD				
6.1 ORGANIZACIÓN INTERNA	Si	No		
6.1.1 Comité de gestión de Seguridad de la información			**Evidencia**	**Observación**
Existe un comité multidisciplinario que apoya activamente al control de la seguridad de la informacion de la organización		X	Plan de Seguridad Acta de conformación de comite de gestión Plan del comité de gestion de seguridad de informacion	
6.1.2. Coordinacion de la Seguridad de la informacion			**Evidencia**	**Observación**
Existe cooperacion coordinada entre representantes de diferentes areas de la organización para asegurar que las actividades de seguridad sean efectivas	X		Estructura organizacional de la empresa Documento de implementacion de la politica de seguridad de informacion Plan de seguridad Informes de seguridad	
6.1.3. Asignacion de responsabilidades sobre seguridad de la informacion			**Evidencia**	**Observación**
Se han asignado responsabilidades con niveles de autorizacion sobre seguridad de la informacion de los activos, tanto fisico como logico, en concordancia con la informacion de la politica de seguridad.	X		Documento de trazabilidad de responsabilidades. Documento de niveles de autorizacion	
6.1.4 Procesos de autorización de recursos para el tratamiento de la información			**Evidencia**	**Observación**
Existencia de un proceso de autorización y evaluacion para la gestión de cada nuevo recurso	X		Documento de autorización Cuadro de mando de controlx Documentación de flujo de procesos Documento de control patrimonial informatico Documento de autorizacion de uso de equipos informaticos personales	
Existencia del control de compatibilidad del hardware y software con los demas dispositivos del sistema	X		Documento de especificaciones tecnicas, Documento de certificación Documento de compatibilidad	

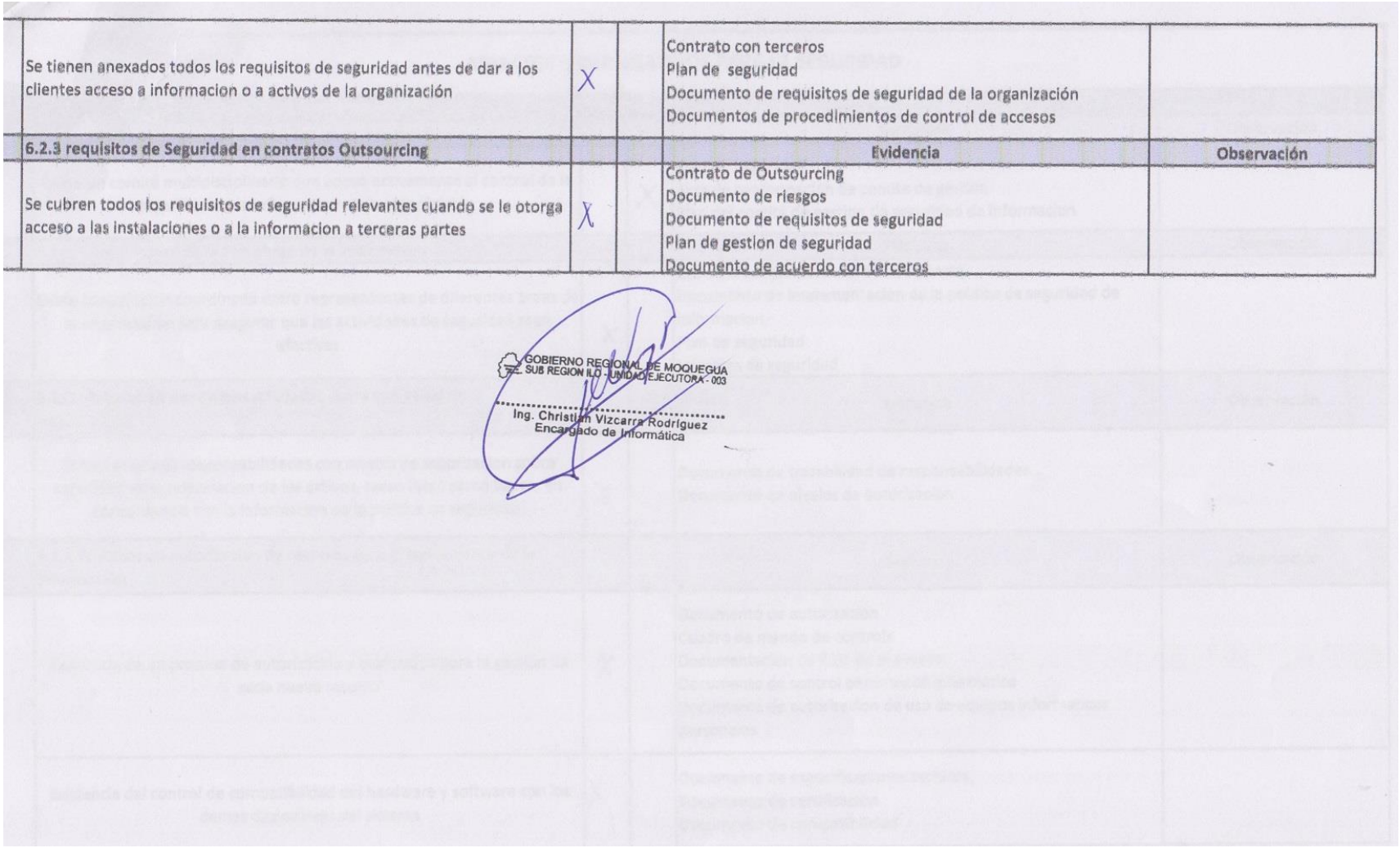
Figura 17

Hoja De Evaluación: Aspectos Organizativos Para La Seguridad 2.

Existencia de autorización y evaluación del uso de medios informáticos personales	X		Documento de control patrimonial informático, Documento de autorización de uso de equipos informáticos personales	
6.1.5 Acuerdos de Confidencialidad			**Evidencia**	**Observación**
Existencia de acuerdos de confidencialidad y de no divulgacion que la organización protege	X		Documentos de acuerdos de confidencialidad Requerimientos de seguridad de la organización Reportes de actualizacion de los acuerdos de confidencialidad	
6.1.6.CONTACTO CON AUTORIDADES			**Evidencia**	**Observación**
La organización tiene procedimientos para contactar con autoridades apropiadas relevantes ante cualquier situacion de seguridad de informacion	X		Documento de requerimientos de seguridad de la organización Documento de canales de comunicación	
6.1.7 CONTACTO CON GRUPOS DE INTERES SOCIAL			**Evidencia**	**Observación**
Constatar que se tengan membresías de grupos de interés especial profesionales u otros especialistas en seguridad	X		Lista de membresías en grupos de interés Documentación de los conocimientos implantados en la organización	
6.1.8. REVISION INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACION			**Evidencia**	**Observación**
El alcance de la organización para gestionar la seguridad de informacion y su implementacion son revisados en intervalos planificados o cuando significativos a la puesta en marcha de la seguridad ocurran	X		Reportes internos Resultados de revisiones indeendientes Documentos de informacion del equipo de individuos ejecutores de la revision	
6.2. SEGURIDAD EN LOS ACCESOS DE TERCERAS PARTES	**Si**	**No**		
6.2.1 Identificación de riesgos por el acceso de terceros - Otra información			**Evidencia**	**Observación**
Existe una evaluacion de riesgos a la informacion de la organización que impliquen a terceros cuando se les concede el acceso a las intalaciones o a la informacion en si.	X		Documento de riesgos y revision de personal Documento de acceso a terceros Documento de obligaciones y responsabilidades de terceros por el acceso provisto	
6.2.2 Requisitos de Seguridad cuando se trata con clientes			**Evidencia**	**Observación**

Figura 18

Hoja De Evaluación: Aspectos Organizativos Para La Seguridad 3



	Se tienen anexados todos los requisitos de seguridad antes de dar a los clientes acceso a informacion o a activos de la organización	X		Contrato con terceros Plan de seguridad Documento de requisitos de seguridad de la organización Documentos de procedimientos de control de accesos	
	6.2.3 requisitos de Seguridad en contratos Outsourcing			**Evidencia**	**Observación**
	Se cubren todos los requisitos de seguridad relevantes cuando se le otorga acceso a las instalaciones o a la informacion a terceras partes	X		Contrato de Outsourcing Documento de riesgos Documento de requisitos de seguridad Plan de gestion de seguridad Documento de acuerdo con terceros	

GOBIERNO REGIONAL DE MOQUEGUA
SUB REGION ILO - UNIDAD EJECUTORA - 003

Ing. Christian Vizcarra Rodriguez
Encargado de Informática

Anexo 03

Figura 19

Hoja de Evaluación: Clasificación y control de activos

CLASIFICACION Y CONTROL DE ACTIVOS

	7.1 RESPONSABILIDAD SOBRE LOS ACTIVOS	SI	NO		
7.1.1	**INVENTARIO DE ACTIVOS**			**Evidencia**	**Observación**
	Los activos de la organización, tanto fisicos como logicos, estan identificados y clasificados bajo el nivel de importancia, valor y seguridad.	X		Documento de Identificacion de activos Inventario de activos	
7.1.2	**PROPIEDAD DE LOS ACTIVOS**			**Evidencia**	**Observación**
	Se han asignado responsabilidades de propiedad de activos, tanto fisico como logicos y toda la informacion asociada por parte de la organización.	X		Documento de Responsabilidad sobre activos Documento de asignacion de propiedad sobre activos	
7.1.3	**USO ADECUADOS DE ACTIVOS**			**Evidencia**	**Observación**
	Cuenta con medidas y reglas en torno al uso de internet y aparatos moviles para el uso adecuado de activos	X		Guias provistas por la Gerencia sobre el uso adecuado de los activos	
	7.2 CLASIFICACION DE LA INFORMACION	SI	NO		
7.2.1	**GUIAS DE CLASIFICACION**			**Evidencia**	**Observación**
	Se ha clasificado la informacion de los activos en grados de prioridades y proteccion en funcion de su valor, requisitos legales, sensibilidad y criticidad para la organización	X		Documento de Clasificacion de Activos Politicas de control de activos Documento de analisis de impacto	
7.2.2	**MARCADO Y TRATAMIENTO DE LA IINFORMACION**			**Evidencia**	**Observación**
	Existen procedimientos para marcar y tratar la informacion como sensible o critica según el esquema de clasificacion adoptado por la organización.	X		Manual de Procedimientos Acuerdos de informacion compartida Politicas y normas de gestion de la informacion Registro de etiquetas de informacion de la organización	

GOBIERNO REGIONAL DE MOQUEGUA
SUB REGIONAL ILO - UNIDAD EJECUTORA-003
Abog. EMILIO ENCALADA OLAVARRIA
Jefe de Oficina Sub Regional de Administración

Anexo 04

Figura 20

Hoja de evaluación: Seguridad en recursos humanos 1

SEGURIDAD EN RECURSOS HUMANOS

1	Seguridad Antes del Empleo	SI	NO		
1.1	**Inclusión de la seguridad en las responsabilidades y funciones laborales**			**EVIDENCIA**	**OBSERVACION**
	Estas definidas y documentadas las funciones y responsabilidades de los empleados, contratistas y terceros en concordancia con la politica de seguridad de la organización	X		Políticas de seguridad Documento de funciones y responsabilidades Registro de comunicación de funciones y responsabilidades	
1.2	**Selección y política de personal**			**EVIDENCIA**	**OBSERVACION**
	Se verifican los datos del candidato para el empleo, en concordancia con las leyes, regulaciones y la etica	X		Listas de verificacion Procesos de seleccion Procesos de selección de personal Legislacion acerca de contrato de personal Acuerdos con agencias terceras	
1.3	**Acuerdos de confidencialidad**			**EVIDENCIA**	**OBSERVACION**
	El empleado, contratista o tercero, ademas de la organización, poseen obligaciones bajo los terminos y condiciones del contrato de empleo	X		Acuerdos contractuales Terminos y condiciones del empleo Codigos de conducta	
2	Durante el Empleo	SI	NO		
2.1	**Responsabilidades de la gerencia**			**EVIDENCIA**	**OBSERVACION**
	La organización requiere empleados, contratistas y usuarios de terceros, en forma adecuada, para aplicar la seguridad en concordancia con las politicas y los procedimientos de la misma	X		Manual de Organización y Funciones Charlas de motivacion, insentivos Evaluacion, cuestionarios Evaluadores de desempeños Politicas de seguridad	
2.2	**Conocimiento, educación y entrenamiento de la seguridad de información**			**EVIDENCIA**	**OBSERVACION**
	Los empleados, contratistas o usuaruis de terceros reciben enternamiento apropiado en politicas y procedimientos organizacionales relevantes para la funcion que desempeñan	X		Fotografias, evaluacion de capacitacion, listas de asistencias, afiches y tripticos	
2.3	**Proceso disciplinario**			**EVIDENCIA**	**OBSERVACION**

Figura 21

Hoja de evaluación: Seguridad en recursos humanos 2

	Existe un proceso formal disciplinario para empleados que han cometido una apertura en la seguridad de la informacion de la organización		X	Políticas y procedimientos organizacionales de seguridad Contratos de empleados Procedimientos del proceso disciplinario Codigos de conducta	
3	Finalización o cambio de empleo	SI	NO		
3.1	Responsabilidades de finalización			EVIDENCIA	OBSERVACION
	El termino de un empleo o el cambio de este, estan claramente definidas y asignadas	X		Procedimientos de seguridad relevantes Terminos y condiciones para los puestos y cargos Procedimientos d finalizacion de responsabilidades Acta de entrega de cargo	
3.2	Retorno de activos			EVIDENCIA	OBSERVACION
	Existen procedimientos para que los empleados, contratistas y terceros retornen los activos de la organización cuando la finalizacion del empleo, contrato o acuerdo finalice.	X		Entrega de Cargo Acta de Informe de Gestion Manual de procedimientos	
3.3	Retiro de los derechos de acceso.			EVIDENCIA	OBSERVACION
	Existen procedimientos para remover los accesos a los empleados, contratistas o usuarios de terceros cuando el empleo, contrato o acuerdo culmine.	X		Manual de Procedimientos Informe de la oficina de acceso	

GOBIERNO REGIONAL DE MOQUEGUA
SUB REGIÓN ILO - UNIDAD EJECUTORA-303

Abog. EMILIO ENCALADA OLAVARRIA
Jefe de Oficina Sub Regional de Administración

Anexo 05

Figura 22

Hoja de evaluación: Seguridad física y del entorno 1

SEGURIDAD FISICA Y DEL ENTORNO					
9,1	áreas seguras	Si	No	Evidencia	OBSERVACIÓN
	Se evita los accesos no autorizados, daños e interferencias contra los locales y la información de la organización	X		política de seguridad, plan de contingencia.	
	Los recursos para el tratamiento de información sensible para la organización se encuentran ubicados en áreas seguras con barreras de seguridad y controles de entrada apropiados.	X		política de seguridad, plan de contingencia,planos.	
	Existe protección física contra accesos no autorizados, daños e interferencias.	X		política de seguridad, plan de contingencia,planos.	
9.1.1	Perímetro de seguridad física	Si	No	Evidencia	OBSERVACIÓN
	El perímetro de seguridad esta claramente definido y el lugar y fuerza de cada perímetro depende de los requerimientos de seguridad del activo entre el perímetro y los resultados de la evaluación de riesgos.	X		política de seguridad, plan de contingencia,planos.	
	Los muros externos del lugar son sólidos y las puertas y ventanas exteriores estan protegidas contra accesos no autorizados.	X		política de seguridad, plan de contingencia,planos.	
	Existe un área de recepción manual u otros medios de control del acceso físico al edificio o lugar. Se restrinje el ingreso sólo al personal autorizado.	X		política de seguridad, plan de contingencia,planoslibro de control de personal.	
	Las puertas para incendios del perímetro de seguridad tienen alarma, son monitoreadas, probadas y operan en concordancia con el código de fuego local como una forma de seguridad.		X	política de seguridad, plan de contingencia,planos,sistemas de seguridad.	
	Existen sistemas adecuados de detección de intrusos de acuerdo a estándares regionales, nacionales o internacionales y son regularmente probados para cubrir todas las puertas externas y ventanas de acceso.		X	política de seguridad, plan de contingencia,planos,sistemas de seguridad.	
	Los recursos de procesamiento de información manejadas por la organización estan físicamente separados de los que son manejados por terceros.	X		política de seguridad, plan de contingencia,planos,informes,documentos con autorizacion.	
9.1.2	Controles físicos de entradas	Si	No	Evidencia	OBSERVACIÓN
	Las áreas de seguridad estan protegidas por controles de entrada adecuados que aseguran el permiso de acceso sólo al personal autorizado.		X	política de seguridad, plan de contingencia,planos,informes,documentos con autorizacion,sistemas de seguridad.	

Figura 23

Hoja de evaluación: Seguridad física y del entorno 2

	Las visitas a áreas seguras son supervisadas, o se aprueba el acceso previamente; se registra fecha y momento de entrada y salida.	X		política de seguridad, plan de contingencia,planos,informes,documentos con autorizacion,sistemas de seguridad,manual de procedimientos,señalización .	
	El acceso a la información sensible y a los recursos de su tratamiento es controlado y restringido sólo al personal autorizado .	X		política de seguridad, plan de contingencia,planos,informes,documentos con autorizacion,sistemas de seguridad,manual de procedimientos,señalización .	No existe documento, sólo proceso
	Se utilizan controles de autenticación para autorizar y validar el acceso; se exige alguna forma de identificación visible.		X	política de seguridad, plan de contingencia,planos,informes,documentos con autorizacion,sistemas de seguridad,manual de procedimientos,señalización .	
	Se garantiza el acceso restringido al personal de apoyo de terceros, hacia áreas de seguridad o a los recursos de procesamiento de información sensibles, solo cuando este es requerido. Este acceso es autorizado y monitoreado.	X		política de seguridad, plan de contingencia,planos,informes,documentos con autorizacion,sistemas de seguridad,manual de procedimientos,señalización,registros .	
	Se revisa y actualiza regularmente los derechos de acceso a las áreas de seguridad.	X		política de seguridad, plan de contingencia,informes,documentos con autorizacion,sistemas de seguridad,manual de procedimientos,señalización,registros .	
9.1.3	**Seguridad de oficinas, despachos y recursos**	**Si**	**No**	**Evidencia**	**OBSERVACIÓN**
	se tiene asignada y se aplicada la seguridad física para oficinas, despachos y recursos.	X		política de seguridad, plan de contingencia,informes,documentos con autorizacion,sistemas de seguridad,manual de procedimientos,señalización,registros .	
	se toma en cuenta las regulaciones y estándares de salud y seguridad.	X		política de seguridad, plan de contingencia,informes,documentos con autorizacion,sistemas de seguridad,manual de procedimientos,señalización,registros .	
	Se tiene instalados equipos con clave para evitar el acceso del publico.	X		política de seguridad, plan de contingencia,informes,documentos con autorizacion,sistemas de seguridad,manual de procedimientos,señalización,registros .	
9.1.4	**Protección contra amenazas externas y ambientales**	**Si**	**No**	**Evidencia**	**Observaciones**
	Existen medidas de protección física contra desastres naturales o humanos	X		Documento de política de seguridad e imágenes	

Figura 24

Hoja de evaluación: Seguridad física y del entorno 3

	Los materiales peligrosos y combustibles están almacenados en un lugar distante de las áreas seguras		X	Documento de política de seguridad e imágenes	
	El equipo y los medios de respaldo están a una distancia de seguridad conveniente	X		Documento de política de seguridad e imágenes	
	Existen equipos adecuados contra incendios	X		Documento de política de seguridad, imágenes, informe de la compra de equipos	
9.1.5	**El trabajo en las áreas seguras**	**Si**	**No**	**Evidencia**	**Observaciones**
	Existe un diseño de protección física y pautas para trabajar en áreas seguras	X		Documento de política de seguridad, Plano y Certificado de Funcionamiento	físicamente sí
	El personal conoce la existencia de un área segura y las actividades de seguridad	X		Documento de política de seguridad y una encuesta o grabación de encuesta verbal	
	Hay supervisión del trabajo en áreas seguras		X	Documento de política de seguridad e imágenes (reglamento)	
	Exsite un control periódico de las áreas seguras cuando están vacías		X	Documento de política de seguridad e imágenes	
	Hay una política que restringe la presencia de equipos de fotografía, video, audio u otras formas, salvo autorización especial	X		Documento de política de seguridad e imágenes, video o documento de autorizacción (procedimiento)	No escrito, sólo memorandums
9.1.6	**Acceso público, áreas de carga y descarga**	**Si**	**No**	**Evidencia**	**Observaciones**
	Existe un control de las áreas de carga y descarga	X		Documento de política de seguridad e imágenes	
	Existe la aislación de los recursos de tratamiento de información para evitar accesos no autorizados	X		Documento de política de seguridad e imágenes	
	Existe una política de restricción a los accesos del área de carga y descarga desde el exterior, únicamente al personal autorizado e identificado	X		Documento de política de seguridad e imágenes o ducumento de autorización (procedimiento)	
	Existe un diseño de área de carga y descarga para que los suministros puedan descargarse sin tener acceso a otras zonas del edificio	X		Documento de política de seguridad, Plano Y Certificado de Funcionamiento	
	Existe inspección del material entrante antes de llevarlo a su lugar de utilización	X		Documento de política de seguridad, imágenes e informe de material entrante	
	Está físicamente separado el material entrante y saliente ,donde sea posible.	X		Documento de política de seguridad e imágenes	
9.2	**Seguridad de los equipos**	**Si**	**No**	**Evidencia**	**Observaciones**
	Existen medidas para evitar daños/pérdidas que comprometan los activos de la organización	X		Documento de política de seguridad	
	Existen medidas para evitar la interrupción de actividades de la organización	X		Documento de política de seguridad	
	Existen equipos físicamente protegidos de amenazas	X		Documento de política de seguridad e imágenes	

Figura 25

Hoja de evaluación: Seguridad física y del entorno 4

	Existe la disponibilidad de equipos	X		Documento de política de seguridad e imágenes	
	Hay una buena instalación de equipos	X		Documento de política de seguridad e imágenes	
	Existen medidas y controles especiales contra riesgos de accesos no autorizados para proteger los sistemas de apoyo	X		Documento de política de seguridad	
	Existen medidas y controles especiales contra riesgos de accesos no autorizados para proteger la alimentación interrumpida e infraestructura del cableado	X		Documento de política de seguridad e imágenes	
9.2.1	**Instalación y protección de equipos**	**SI**	**No**	**Evidencia**	**Observaciones**
	Existen equipos situados de forma segura			Documento de política de seguridad e imágenes	
	Están protegidos los equipos de amenazas del entorno y de acceso no autorizados	X		Documento de política de seguridad e imágenes	
	Están instalados los equipos de tratamiento y almacenamiento de información sensible en un lugar que no permite la observación de personas no autorizados en el área de trabajo	X		Documento de política de seguridad e imágenes	
	Están aislados los elementos que requieren especial protección	X		Documento de política de seguridad e imágenes	
	Existen controles para minimizar el riesgo de amenzas externas	X		Documento de política de seguridad e imágenes	
	Existen políticas sobre fumar, beber y comer cerca de los equipos de tratamiento de información	X		Documento de política de seguridad e imágenes	No esta escrita, guía según ley N°276
	Existe vigilación de las condiciones ambientales, como temperatura y humedad que afecten el funcionamiento de equipos de tratamiento de información		X	Documento de política de seguridad e imágenes	
	Existe ajustes de filtro de luz en todas las líneas de poder y comunicación			Documento de política de seguridad e imágenes	
	Existen métodos de protección especial para los equipos situados en ambientes industriales		X	Documento de política de seguridad e imágenes	
9.2.2	**Suministro eléctrico**	**SI**	**NO**	**EVIDENCIA**	**OBSERVACIÓN**
	Existe una adecuada Instalacion de apoyo para el suministro eléctrico de los equipos informáticos (electricidad, el suministro de agua, desagüe, calefacción/ventilación y aire acondicionado)	X		Planos eléctricos, planos del tuberías eléctricas, instalación de pozo tierra	
	Existe instalado un Sistema de Alimentación Ininterrumpida (U.P.S.)	X		plan de contingencia, informe de instalación	
	Existe un generador de respaldo.		X	plan de contingencia	

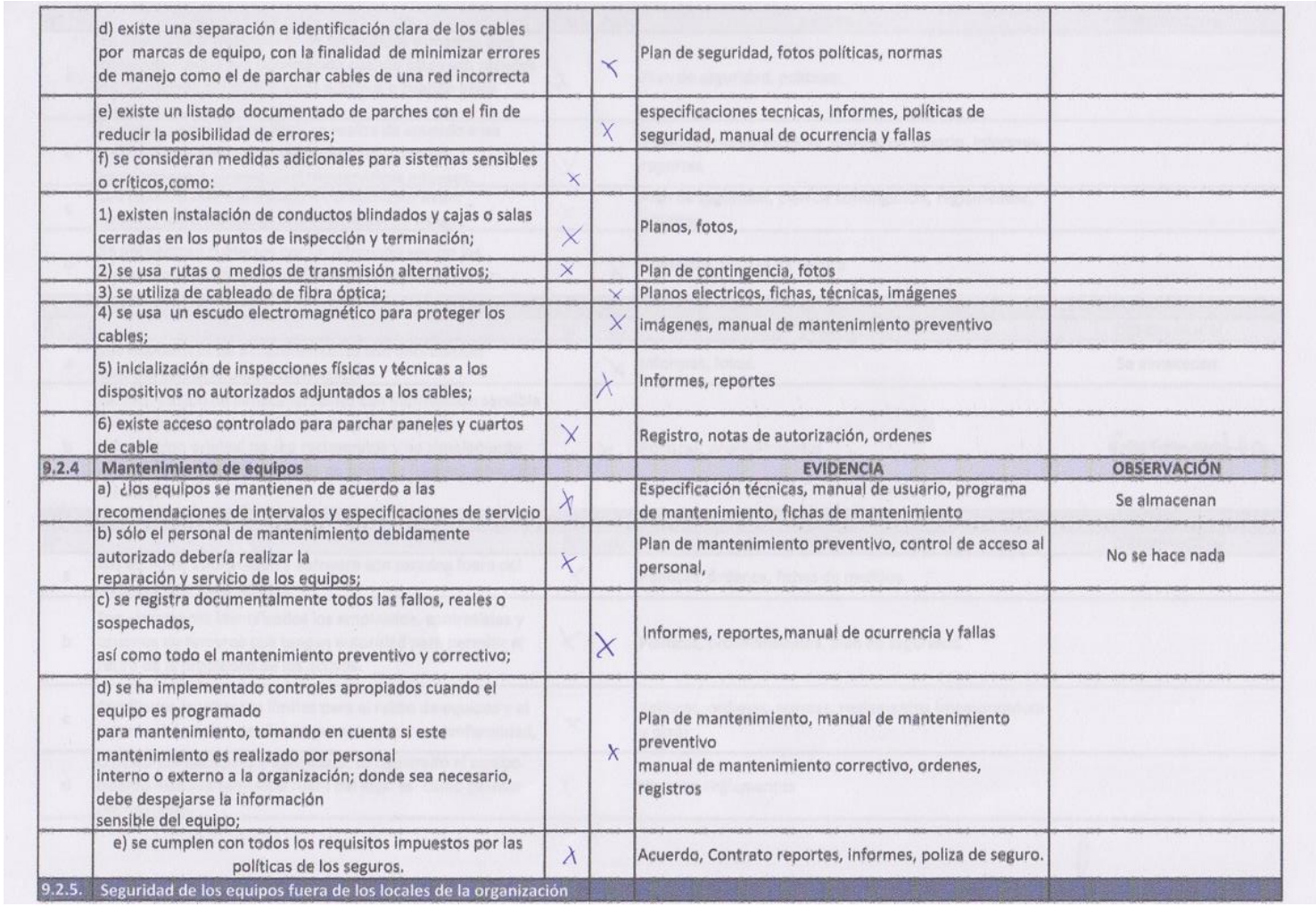
Figura 26

Hoja de evaluación: Seguridad física y del entorno 5

	Se establecieron prueba de control sobre el funcionamiento de los equipos de acuerdo a recomendaciones del fabricante	X		Manual del equipo	
	Existen un control en el abastecimiento de combustible para el funcionamiento del generador durante periodos prolongados		X	Plan de contingencia,	
	Se tiene en consideración el uso de múltiples fuentes de poder o si el lugar es amplio, una subestación de poder separada.		X	Planos, plan de contingencia	
	Existen interruptores de emergencia cerca de las puertas de emergencia de las salas de equipos para facilitar una desconexión rápida en caso de emergencia. Por si falla la energía se dispone de alumbrado de emergencia.		X	Planos plan de contingencia	
	El estable el suministro de agua y adecuado para suministrar aire acondicionado, equipos de humidificación y sistemas contra incendios (donde sean utilizados).		X	Plan de seguridad, Plan de contingencia , imágenes de las reserva de agua	
	Existe un sistema de alarma para detectar problemas de funcionamiento en las instalaciones de apoyo. si es así, se hizo la evaluación e instalación requerida		X	Plan de contingencia, plan de seguridad, plano, informes, fotos	
	Existen equipos de telecomunicación existe la conexión al proveedor al menos por dos rutas para prevenir la falla en una conexión eliminando el servicio de voz. Este servicio debe ser adecuado para satisfacer requisitos locales legales para comunicaciones de emergencia.		X	Plan de contingencia	
9.2.3	**Seguridad del cableado**	**SI**	**NO**	**EVIDENCIA**	**OBSERVACIÓN**
	a) las líneas de energía y telecomunicaciones en las zonas de tratamiento de información, encuentra enterradas, o adoptan medidas alternativas de protección	X		Planos electricos, manual de mantenimiento electrico, manual de ocurrencia y fallas	
	b) la red cableada se está protegida contra intercepciones no autorizadas o daños, por ejemplo, usando conductos y evitando rutas a través de áreas públicas;	X		Planos electricos, manual de mantenimiento electrico, fotos	
	c) se encuentran separados los cables de energía de los de comunicaciones para evitar interferencias;	X		manual de mantenimiento electrico Planos electricos, especificaciones tecnicas, fotos	

Figura 27

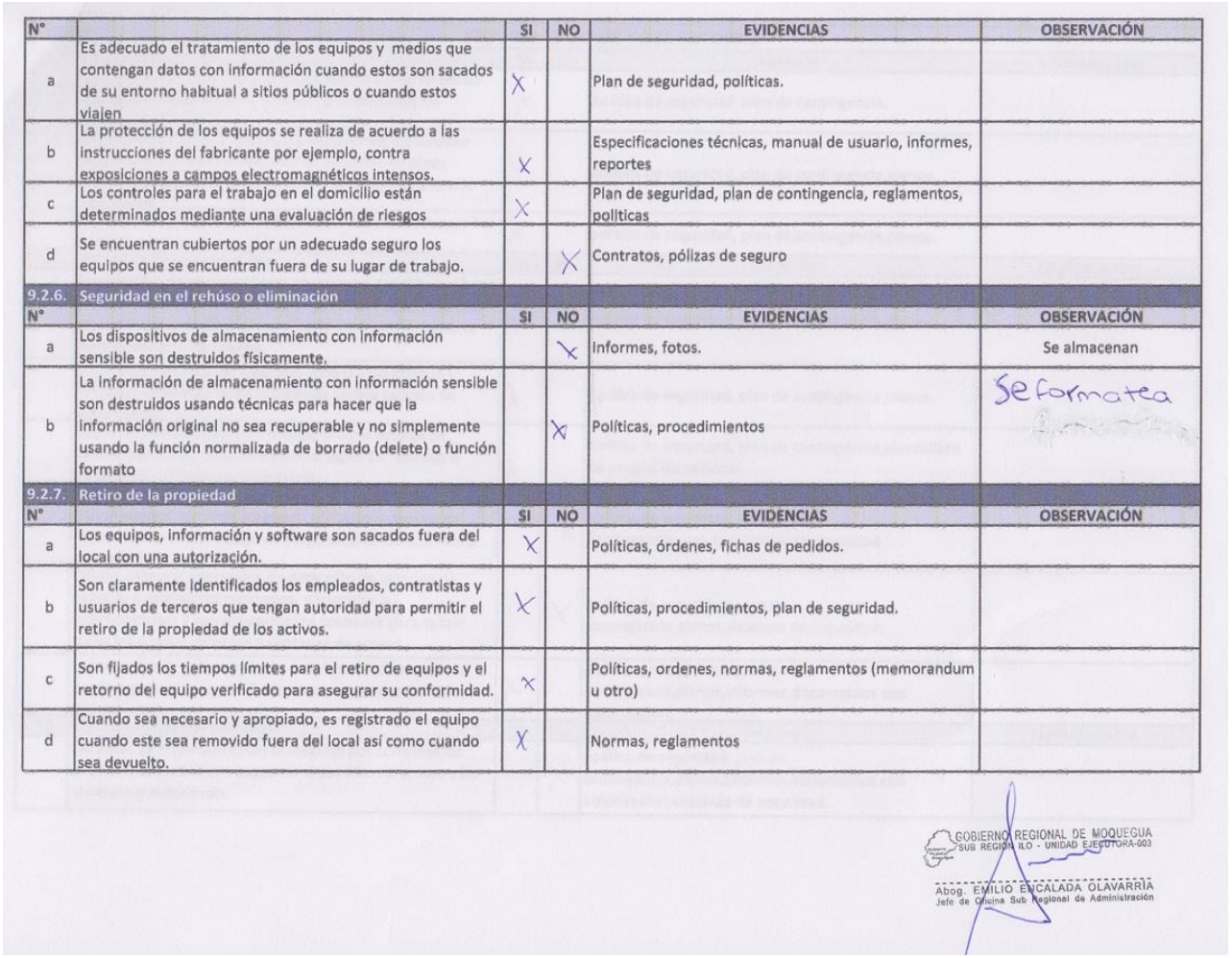
Hoja de evaluación: Seguridad física y del entorno 6



	d) existe una separación e identificación clara de los cables por marcas de equipo, con la finalidad de minimizar errores de manejo como el de parchar cables de una red incorrecta		X	Plan de seguridad, fotos políticas, normas	
	e) existe un listado documentado de parches con el fin de reducir la posibilidad de errores;		X	especificaciones tecnicas, Informes, políticas de seguridad, manual de ocurrencia y fallas	
	f) se consideran medidas adicionales para sistemas sensibles o críticos,como:	X			
	1) existen instalación de conductos blindados y cajas o salas cerradas en los puntos de inspección y terminación;	X		Planos, fotos,	
	2) se usa rutas o medios de transmisión alternativos;	X		Plan de contingencia, fotos	
	3) se utiliza de cableado de fibra óptica;		X	Planos electricos, fichas, técnicas, imágenes	
	4) se usa un escudo electromagnético para proteger los cables;		X	imágenes, manual de mantenimiento preventivo	
	5) inicialización de inspecciones físicas y técnicas a los dispositivos no autorizados adjuntados a los cables;		X	Informes, reportes	
	6) existe acceso controlado para parchar paneles y cuartos de cable	X		Registro, notas de autorización, ordenes	
9.2.4	**Mantenimiento de equipos**			**EVIDENCIA**	**OBSERVACIÓN**
	a) ¿los equipos se mantienen de acuerdo a las recomendaciones de intervalos y especificaciones de servicio	X		Especificación técnicas, manual de usuario, programa de mantenimiento, fichas de mantenimiento	Se almacenan
	b) sólo el personal de mantenimiento debidamente autorizado debería realizar la reparación y servicio de los equipos;	X		Plan de mantenimiento preventivo, control de acceso al personal,	No se hace nada
	c) se registra documentalmente todos las fallos, reales o sospechados, así como todo el mantenimiento preventivo y correctivo;		X	Informes, reportes,manual de ocurrencia y fallas	
	d) se ha implementado controles apropiados cuando el equipo es programado para mantenimiento, tomando en cuenta si este mantenimiento es realizado por personal interno o externo a la organización; donde sea necesario, debe despejarse la información sensible del equipo;		X	Plan de mantenimiento, manual de mantenimiento preventivo manual de mantenimiento correctivo, ordenes, registros	
	e) se cumplen con todos los requisitos impuestos por las políticas de los seguros.	X		Acuerdo, Contrato reportes, informes, poliza de seguro.	
9.2.5.	Seguridad de los equipos fuera de los locales de la organización				

Figura 28

Hoja de evaluación: Seguridad física y del entorno 7



N°		SI	NO	EVIDENCIAS	OBSERVACIÓN
a	Es adecuado el tratamiento de los equipos y medios que contengan datos con información cuando estos son sacados de su entorno habitual a sitios públicos o cuando estos viajen	X		Plan de seguridad, políticas.	
b	La protección de los equipos se realiza de acuerdo a las instrucciones del fabricante por ejemplo, contra exposiciones a campos electromagnéticos intensos.	X		Especificaciones técnicas, manual de usuario, informes, reportes	
c	Los controles para el trabajo en el domicilio están determinados mediante una evaluación de riesgos	X		Plan de seguridad, plan de contingencia, reglamentos, políticas	
d	Se encuentran cubiertos por un adecuado seguro los equipos que se encuentran fuera de su lugar de trabajo.		X	Contratos, pólizas de seguro	
9.2.6.	Seguridad en el rehúso o eliminación				
N°		SI	NO	EVIDENCIAS	OBSERVACIÓN
a	Los dispositivos de almacenamiento con información sensible son destruidos físicamente.		X	Informes, fotos.	Se almacenan
b	La información de almacenamiento con información sensible son destruidos usando técnicas para hacer que la información original no sea recuperable y no simplemente usando la función normalizada de borrado (delete) o función formato		X	Políticas, procedimientos	Se formatea
9.2.7.	Retiro de la propiedad				
N°		SI	NO	EVIDENCIAS	OBSERVACIÓN
a	Los equipos, información y software son sacados fuera del local con una autorización.	X		Políticas, órdenes, fichas de pedidos.	
b	Son claramente identificados los empleados, contratistas y usuarios de terceros que tengan autoridad para permitir el retiro de la propiedad de los activos.	X		Políticas, procedimientos, plan de seguridad.	
c	Son fijados los tiempos límites para el retiro de equipos y el retorno del equipo verificado para asegurar su conformidad.	X		Políticas, ordenes, normas, reglamentos (memorandum u otro)	
d	Cuando sea necesario y apropiado, es registrado el equipo cuando este sea removido fuera del local así como cuando sea devuelto.	X		Normas, reglamentos	

GOBIERNO REGIONAL DE MOQUEGUA
SUB REGIÓN ILO - UNIDAD EJECUTORA-003

Abog. EMILIO ESCALADA OLAVARRIA
Jefe de Oficina Sub Regional de Administración

Anexo 06

Figura 29

Hoja de evaluación: Gestión de Comunicaciones y operaciones 1

GESTION DE COMUNICACIONES Y OPERACIONES

10.1	Procedimientos y Responsables de Operación	SI	NO		
10.1.1	**DOCUMENTACION DE PROCEDIMINETOS OPERATIVOS**			**Evidencia**	**Observacion**
	existen procesos y utilización correcta de la información	X		procedimiento para la administracion del sistema	
	existen las instrucciones para manejar errores u otras condiciones excepcionales que puedan ocurrir durante la tarea de ejecución		X	procedimientos para procesamiento de informacion	
	existe un plan de seguridad para el reinicio del sistema y los procedimientos de recuperación a utilizar en caso de fallo del sistema.	X		procedimiento para la administracion del sistema	
	existe la gestión de la información del rastro de auditoria y del registro de sistema en los documentos de gestion	X		procedimientos para procesamiento de informacion	
10.1.2	**GESTION DE CAMBIOS**			**Evidencia**	**Observacion**
	existe la identificación y registro de cambios significativos.	X		Responsabilidades y procedimientos de gestión de cambios.	en servidores.
	existe planeamiento y prueba de los cambios.	X		Responsabilidades y procedimientos de gestión de cambios.	
	existe un procedimiento formal para la aprobación de los cambios propuestos.	X		Responsabilidades y procedimientos de gestión de cambios.	
	existe la comunicación de los detalles de cambio a todas las personas que corresponda.	X		responsabilidades y procedimeintos de gestion de cambios	
	existen procedimientos que identifiquen las responsabilidades de abortar y recobrarse de los cambios sin éxito	X		responsabilidades y procedimeintos de gestion de cambios	
10.1.3	**SEGREGACION DE TAREAS**			**Evidencia**	**Observacion**
	se tiene cuidado del personal que puede acceder, modificar o utilizar los activos sin autorización o sin ser detectado	X		Documento de segregación de tareas	
	Se verifica que la iniciación de un evento debe estar separada de su autorización		X	Documento de segregación de tareas	
10.1.4	**SEPARACION DE LOS RECURSOS PARA DESARROLLO Y PARA PRODUCCION**			**Evidencia**	**Observacion**
	Se puede comprobar si existen perfiles de usuarios para el uso del sistemas operacionales, los menus deben de exhibir mensajes de identificacion apropiados para reducir el riesgo por error	X		Documento de controles para el nivel de separación de entornos.	
10.2	**GESTION DE SERVICIOS EXTERNOS**				

Figura 30

Hoja de evaluación: Gestión de Comunicaciones y operaciones 2

10.2.1	SERVICIO DE ENTREGA			Evidencia	Observacion
	se verifica que el servicio entregado por terceros incluye los arreglos de seguridad acordados	X		documento de contratos con terceros sobre seguridad	No se trabaja con terceros
	se verifica planes realizables designados de la organización se asegure que los terceros mantengan una capacidad suficiente para asegurar que los niveles continuos del servicio acordado sean mantenidos siguiendo fallas mayores del servicio o desastre		X	Constancia de capacidad suficiente por parte de terceros.	
10.2.2	MONITOREO Y REVISION DE LOS SERVICIOS EXTERNOS			Evidencia	Observacion
	Se hace la verificacion de los reportes de revisión de servicio producidos por terceros y que arregle reuniones regulares de progreso como requieran los acuerdos		X	Acuerdos firmados con terceros	
	Se hace la constatacion de la disponibilidad de habilidades y recursos suficientes para monitorear los requisitos de los acuerdos	X		procedimientos en caso de deficiencias en el servicio entregado	
	Se verifica si se han tomado acciones apropiadas cuando se observan deficiencias en el servicio entregado	X		procedimientos en caso de deficiencias en el servicio entregado	
	se verifica el mantenimiento de un control y una visión general suficiente en todos los aspectos para información sensible o crítica o a los recursos del procesamiento de información accedidos	X		procedimientos en caso de deficiencias en el servicio entregado	
10.2.3	GESTIONANDO CAMBIOS PARA LOS SERVICIOS EXTERNOS			Evidencia	Observacion
	existen nuevos controles para resolver incidentes en la seguridad de información y para mejorar la seguridad.	X		Documento de política de seguridad de información.	
	se verifica cambios realizados y realce en las redes.	X		Documento de política de seguridad de información.	
	Se verifica el uso de nuevas tecnologías.	X		Documento de política de seguridad de información.	
	Se verifica si se ha implementado nuevas herramientas y ambientes de desarrollo	X		Documento de política de seguridad de información.	
	Se verifica se ha realizado cambios en la locación física de los recursos de servicio.	X		Documento de política de seguridad de información.	
10.3	PLANIFICACION Y ACEPTACION DEL SISTEMA	SI	NO		
10.3.1	PLANIFICACION DE LA CAPACIDAD			Evidencia	Observacion
	se verifica que se aplicar el monitoreo de los sistemas.	X		documento de implementacion de controles de deteccion	

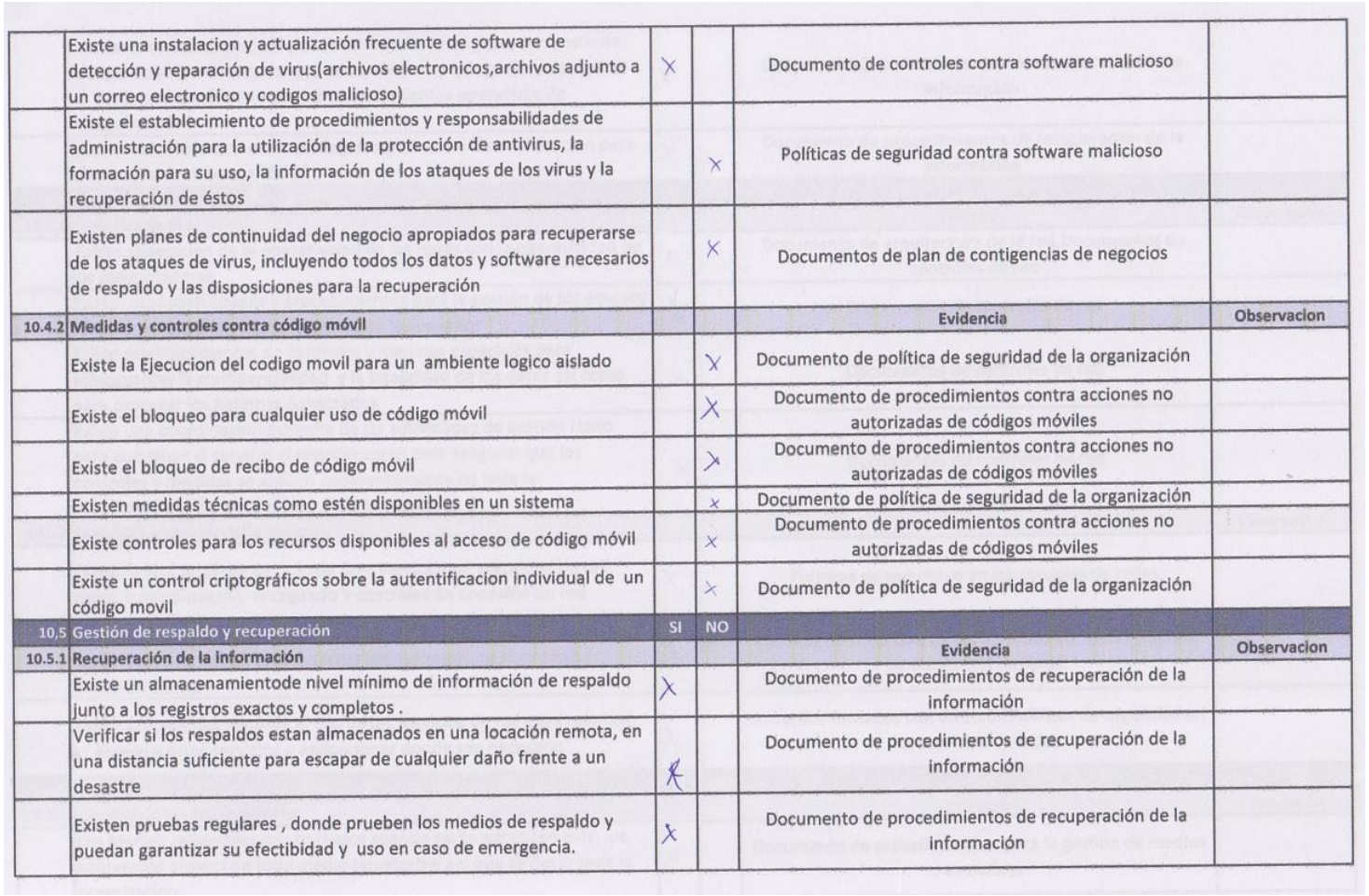
Figura 31

Hoja de evaluación: Gestión de Comunicaciones y operaciones 3

	se comprueba la instalación de controles de detección para detectar los problemas en un tiempo debido.	X		documento de implementacion de controles de deteccion	
	Se hace la constatacion que los administradores usan las tendencias de uso para identificar y evitar posibles cuellos de botella que puedan representar una amenaza	X		Reportes de tendencias de uso	
10.3.2	**ACEPTACION DEL SISTEMA**			**Evidencia**	**Observacion**
	se verifica que los requisitos y criterios de aceptación de los nuevos sistemas están claramentes definidos, acordados, documentados y probados	X		Documento de criterios de aceptación del sistema	
	Se constata que los nuevos sistemas, actualizaciones y las nuevas versiones son migradas a producción solamente después de obtener una aceptación formal.	X		Documentos de requisitos de aceptación del sistema.	
	Se comprueba los requisitos de rendimiento y capacidad de los computadores.	X		Documentos de requisitos de aceptación del sistema.	
	Se comprueba si el manual de procedimiento eficaz.	X		Documentos de requisitos de aceptación del sistema.	
	Se comprueba las evidencias de que la instalación del nuevo sistema no producirá repercusiones negativas sobre los existentes.	X		Documentos de requisitos de aceptación del sistema.	
	Se comprueba la evidencia de que se ha tenido en cuenta el efecto que tendrá el nuevo sistema en la seguridad global de la organización.	X		Documentos de requisitos de aceptación del sistema.	
	Se comprueba que si se realizaron pruebas apropiadas para confirmar que están satisfechas completamente todos los criterios de aceptación	X		documento de conformidad	
10.4	Protección contra software malicioso	SI	NO		
10.4.1	**Medidas y controles contra software malicioso**			**Evidencia**	**Observacion**
	Existen el cumplimiento de licencias de software y la prohibición del uso de software no autorizado	X		Políticas de seguridad contra software malicioso	
	Existen revisiones regulares del software y de los datos contenidos en los sistemas que soportan procesos críticos de la organización,investigandose todo archivo no aprovado y notificaciones no autorizadadas		X	Políticas de seguridad contra software malicioso	

Figura 32

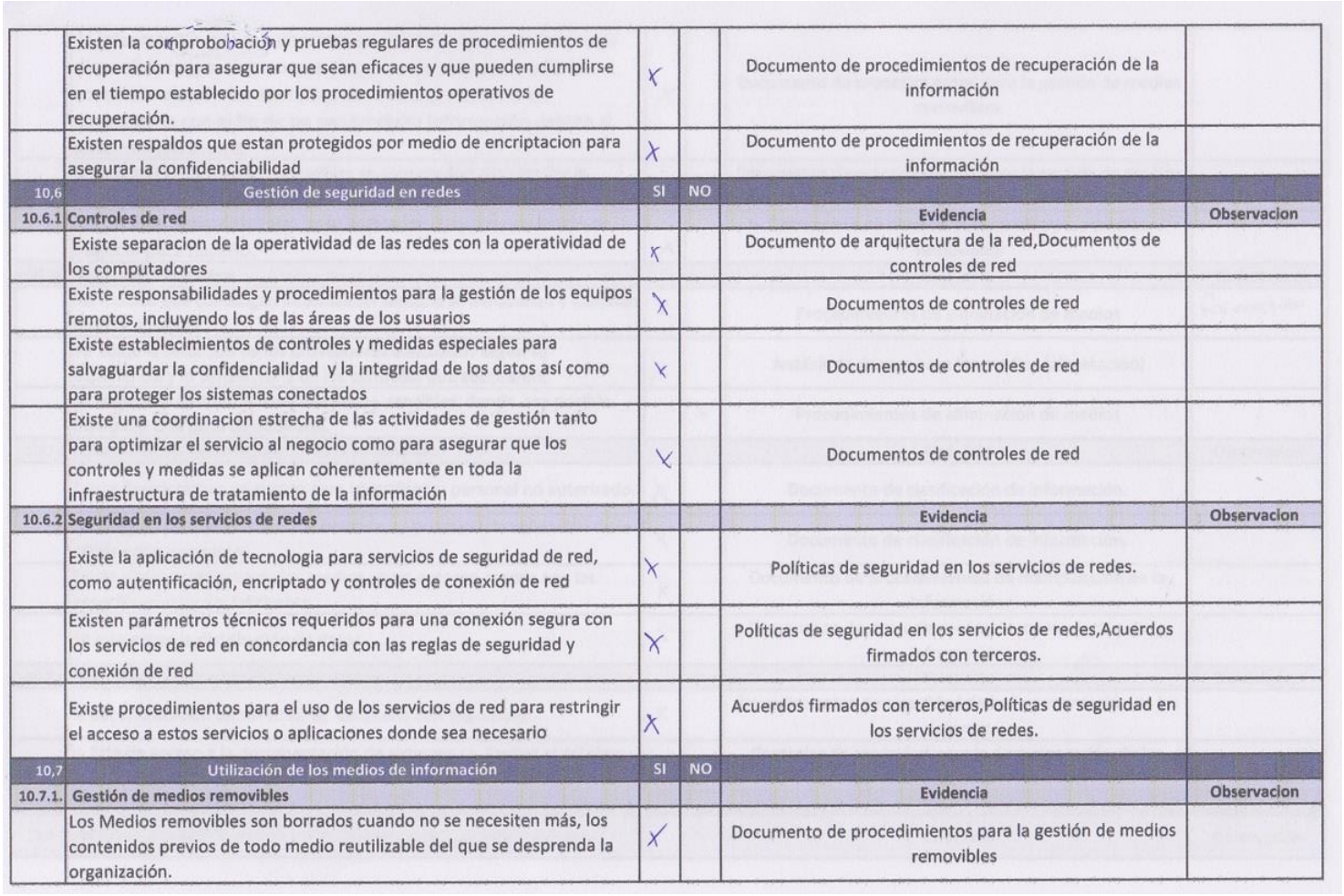
Hoja de evaluación: Gestión de Comunicaciones y operaciones 4



	Existe una instalacion y actualización frecuente de software de detección y reparación de virus(archivos electronicos,archivos adjunto a un correo electronico y codigos malicioso)	X		Documento de controles contra software malicioso	
	Existe el establecimiento de procedimientos y responsabilidades de administración para la utilización de la protección de antivirus, la formación para su uso, la información de los ataques de los virus y la recuperación de éstos		X	Políticas de seguridad contra software malicioso	
	Existen planes de continuidad del negocio apropiados para recuperarse de los ataques de virus, incluyendo todos los datos y software necesarios de respaldo y las disposiciones para la recuperación		X	Documentos de plan de contigencias de negocios	
10.4.2	**Medidas y controles contra código móvil**			**Evidencia**	**Observacion**
	Existe la Ejecucion del codigo movil para un ambiente logico aislado		X	Documento de política de seguridad de la organización	
	Existe el bloqueo para cualquier uso de código móvil		X	Documento de procedimientos contra acciones no autorizadas de códigos móviles	
	Existe el bloqueo de recibo de código móvil		X	Documento de procedimientos contra acciones no autorizadas de códigos móviles	
	Existen medidas técnicas como estén disponibles en un sistema		x	Documento de política de seguridad de la organización	
	Existe controles para los recursos disponibles al acceso de código móvil		x	Documento de procedimientos contra acciones no autorizadas de códigos móviles	
	Existe un control criptográficos sobre la autentificacion individual de un código movil		x	Documento de política de seguridad de la organización	
10,5	Gestión de respaldo y recuperación	SI	NO		
10.5.1	**Recuperación de la información**			**Evidencia**	**Observacion**
	Existe un almacenamientode nivel mínimo de información de respaldo junto a los registros exactos y completos .	X		Documento de procedimientos de recuperación de la información	
	Verificar si los respaldos estan almacenados en una locación remota, en una distancia suficiente para escapar de cualquier daño frente a un desastre	X		Documento de procedimientos de recuperación de la información	
	Existen pruebas regulares , donde prueben los medios de respaldo y puedan garantizar su efectibidad y uso en caso de emergencia.	X		Documento de procedimientos de recuperación de la información	

Figura 33

Hoja de evaluación: Gestión de Comunicaciones y operaciones 5



	Existen la comprobobación y pruebas regulares de procedimientos de recuperación para asegurar que sean eficaces y que pueden cumplirse en el tiempo establecido por los procedimientos operativos de recuperación.	X		Documento de procedimientos de recuperación de la información	
	Existen respaldos que estan protegidos por medio de encriptacion para asegurar la confidenciabilidad	X		Documento de procedimientos de recuperación de la información	
10,6	Gestión de seguridad en redes	SI	NO		
10.6.1	**Controles de red**			**Evidencia**	**Observacion**
	Existe separacion de la operatividad de las redes con la operatividad de los computadores	X		Documento de arquitectura de la red,Documentos de controles de red	
	Existe responsabilidades y procedimientos para la gestión de los equipos remotos, incluyendo los de las áreas de los usuarios	X		Documentos de controles de red	
	Existe establecimientos de controles y medidas especiales para salvaguardar la confidencialidad y la integridad de los datos así como para proteger los sistemas conectados	X		Documentos de controles de red	
	Existe una coordinacion estrecha de las actividades de gestión tanto para optimizar el servicio al negocio como para asegurar que los controles y medidas se aplican coherentemente en toda la infraestructura de tratamiento de la información	X		Documentos de controles de red	
10.6.2	**Seguridad en los servicios de redes**			**Evidencia**	**Observacion**
	Existe la aplicación de tecnologia para servicios de seguridad de red, como autentificación, encriptado y controles de conexión de red	X		Políticas de seguridad en los servicios de redes.	
	Existen parámetros técnicos requeridos para una conexión segura con los servicios de red en concordancia con las reglas de seguridad y conexión de red	X		Políticas de seguridad en los servicios de redes,Acuerdos firmados con terceros.	
	Existe procedimientos para el uso de los servicios de red para restringir el acceso a estos servicios o aplicaciones donde sea necesario	X		Acuerdos firmados con terceros,Políticas de seguridad en los servicios de redes.	
10,7	Utilización de los medios de información	SI	NO		
10.7.1.	**Gestión de medios removibles**			**Evidencia**	**Observacion**
	Los Medios removibles son borrados cuando no se necesiten más, los contenidos previos de todo medio reutilizable del que se desprenda la organización.	X		Documento de procedimientos para la gestión de medios removibles	

Figura 34

Hoja de evaluación: Gestión de Comunicaciones y operaciones 6

	la información que se almaceno en el medio, que requiere estar disponible mayor tiempo que el tiempo de vida del medio (en concordancia con las especificaciones del productor) es almacenada con el fin de no perder dicha información debido al deterioro del medio.	X		Documento de procedimientos para la gestión de medios removibles	
	El registro de los medios removibles es considerado para limitar la oportunidad de perdida de datos.		X	Documento de procedimientos para la gestión de medios removibles	
	los medios removibles son solo activados si existe una razón de negocio para hacerlo.	X		Documento de nivel de autorización para medios removibles	
10.7.2	**Eliminación de medios**			**Evidencia**	**Observacion**
	los medios que contengan información sensible se almacenan y eliminan de forma segura.	X		Procedimientos de eliminación de medios	formateo
	se cuida la selección de los proveedores adecuados según su experiencia y lo satisfactorio de los controles que adoptaron.	X		Análisis de riesgos para los medios (eliminación)	
	Se registra la eliminación de elementos sensibles donde sea posible mantener una pista de auditoria.		X	Procedimientos de eliminación de medios	
10.7.3	**Procedimientos de manipulación de la información**			**Evidencia**	**Observacion**
	Existe Restricciones de acceso para identificar al personal no autorizado.	X		Documento de clasificación de información.	
	Se asegura de que los datos de entrada, su proceso y la validación de la salida están completos.	X		Documento de clasificación de información.	
	Existe almacenamiento de los medios en un entorno acorde con las especificaciones del fabricante.	X		Documento de procedimientos de manipulación de la información	
	Se minimizan la distribución de datos	X		Documento de procedimientos de manipulación de la información	
10.7.4	**Seguridad de la documentación de sistemas**			**Evidencia**	**Observacion**
	la documentación de sistemas se almacena con seguridad.	X		Procedimientos de seguridad de la documentación de los sistemas	
	la lista de acceso a la documentación de sistemas se limitan al máximo, y es autorizada por el propietario de la aplicación.	X		Controles de seguridad para la documentación de los sistemas	
10,8	**Intercambio de información**	**SI**	**NO**		
10.8.1	**Políticas y procedimientos para el intercambio de información y software**			**Evidencia**	**Observacion**

Figura 35

Hoja de evaluación: Gestión de Comunicaciones y operaciones 7

	Existen procedimientos designados para proteger la información intercambiada de una intercepción, copiado, modificación, cambio de ruta y destrucción.	X		Políticas de seguridad sobre conversaciones confidenciales en lugares públicos	
	Existen procedimientos para el uso de comunicaciones inalámbricas, tomando en cuenta los riesgos particulares envueltos;	X		Políticas de seguridad sobre conversaciones confidenciales en lugares públicos	
	Existen responsabilidades de los empleados, contratistas y cualquier otro usuario de no comprometer a la organización, por difamación, hostigamiento, personificación, reenvío de cadenas de correos, compra no autorizada, etc;	X		Políticas de seguridad sobre conversaciones confidenciales en lugares públicos	
	Existe el uso de técnicas criptográficas para proteger la confidencialidad, integridad y autenticidad de la información.	X		Políticas de seguridad sobre conversaciones confidenciales en lugares públicos	
	se deja información critica o sensible en las instalaciones de impresión, como impresoras, copiadoras y faxes, ya que estas pueden ser acezadas por personal no autorizado.		X	Políticas de seguridad sobre conversaciones confidenciales en lugares públicos	
	Se recuerda al personal que deben de tomar precauciones como por ejemplo no revelar información sensible con el fin de evitar ser escuchado o interceptado cuando hagan una llamada telefónica	X		Políticas de seguridad sobre conversaciones confidenciales en lugares públicos	
10.8.2	**Acuerdos de Intercambio**			**Evidencia**	**Observacion**
	Existen responsabilidades de la gerencia para controlar y notificar la transmisión, despacho y recibo.	X		Documentos de acuerdos de intercambio.	
	Existen procedimientos para asegurar al trazabilidad y la no reproducción.		X	Documentos de acuerdos de intercambio.	
	Existen responsabilidades en los eventos de los incidentes de la seguridad de información como la perdida de datos	X		Documentos de acuerdos de intercambio.	
	Existen las propiedades y responsabilidades de la protección de datos, copyright, conformidad de la licencia de software y consideraciones similares	X		Documentos de acuerdos de intercambio.	
10.8.3	**Medios físicos en tránsito**			**Evidencia**	**Observacion**
	Se usan transportes o mensajeros fiables.	X		Procedimientos de transporte de medios informáticos.	

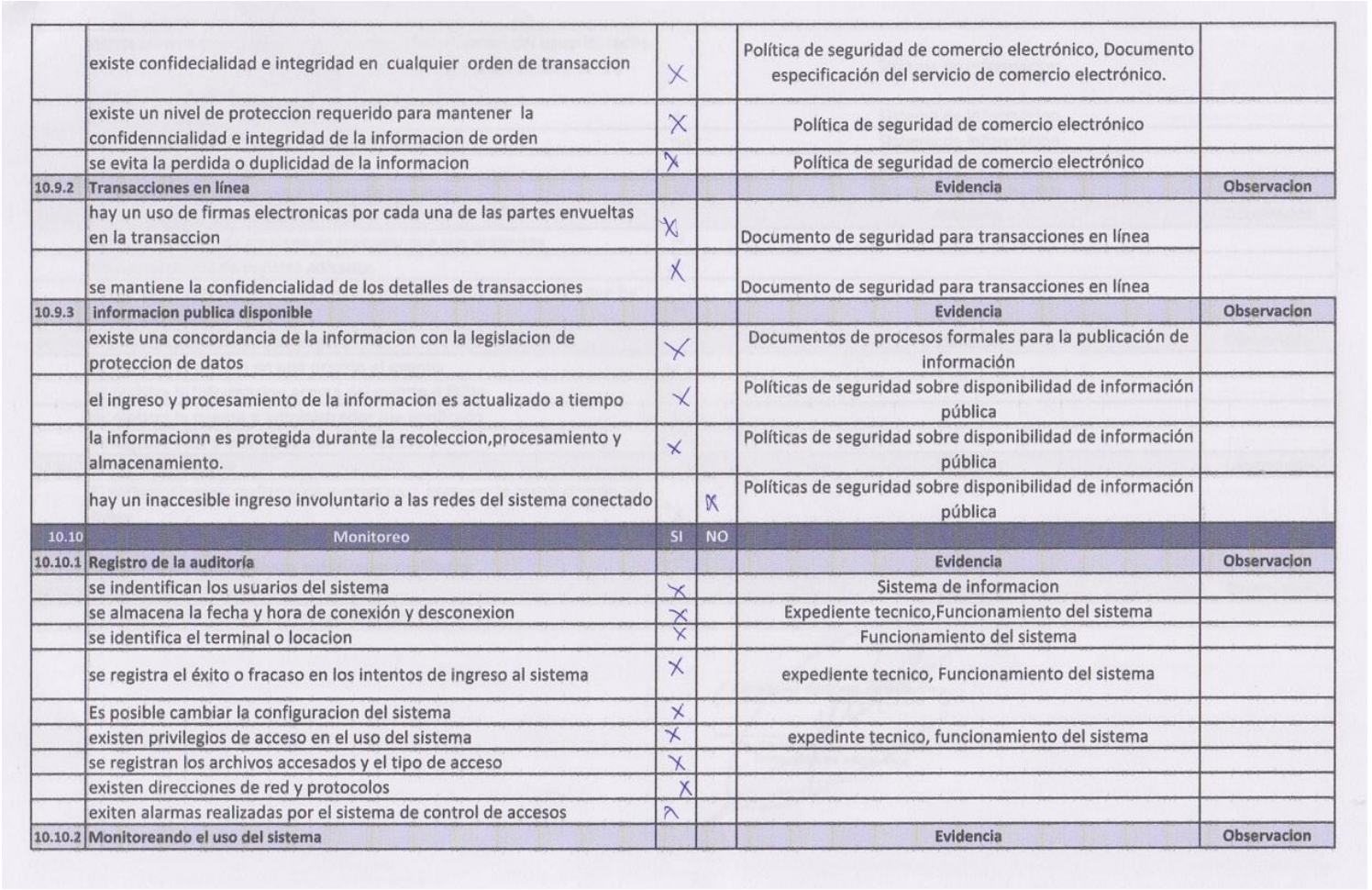
Figura 36

Hoja de evaluación: Gestión de Comunicaciones y operaciones 8

	el envase es suficiente para proteger el contenido contra cualquier daño físico que pueda ocurrir durante el tránsito, por ejemplo protegiéndonos contra cualquier factor ambiental como una exposición al calor, humedad o a campos electromagnéticos.		X	Documento de controles especiales para el transporte de medios informáticos	
10.8.4	**Seguridad en la mensajería electrónica**			**Evidencia**	**Observacion**
	Se asigna una dirección y un transporte correcto del mensaje.	X		Documento de requisitos para firmas electrónicas	
	Existe confiabilidad y disponibilidad general del servicio.	X		Procedimientos para la seguridad en la mensajería electrónica	
	Existen consideraciones legales, por ejemplo los requisitos para firmas electrónicas.	X		Documento de requisitos para firmas electrónicas	
	Existen niveles mas fuertes de autentificación del acceso de control de redes publicas accesibles.	X		Procedimientos para la seguridad en la mensajería electrónica	
10.8.5	**Sistemas de Información de Negocios**			**Evidencia**	**Observacion**
	Existen vulnerabilidades conocidas en los sistemas de administración y contabilidad donde la información es compartida por diferentes partes de la organización.		X	Documento de seguridad para sistemas de información de negocio	
	Existe acceso restringido a la información diaria relacionado con individuos selectos.	X		Documento de interconexión entre sistemas de información de negocio	
	Existen categorías de personal, contratistas o socios de negocios a los que se les permite el uso del sistema y de las locaciones desde donde puede ser accesado		X	Documento de interconexión entre sistemas de información de negocio	
	Se encuentran las instalaciones restringidas seleccionadas para categorías de usuario especificas.	X		Documento de interconexión entre sistemas de información de negocio	
10,9	Servicios de correo electrónico	SI	NO		
10.9.1	**Comercio electrónico**			**Evidencia**	**Observacion**
	existen los requerimientos de confidencialidad, integridad, prueba de despacho y recepcion de documentos clave	X		Política de seguridad de comercio electrónico	
	existe un nivel de confianza requerido en la integridad de la lista de precios anunciadas	X		Documento especificación del servicio de comercio electrónico.	
	existe confidencialidad de cualquier dato o informacion sensible	X		Política de seguridad de comercio electrónico	

Figura 37

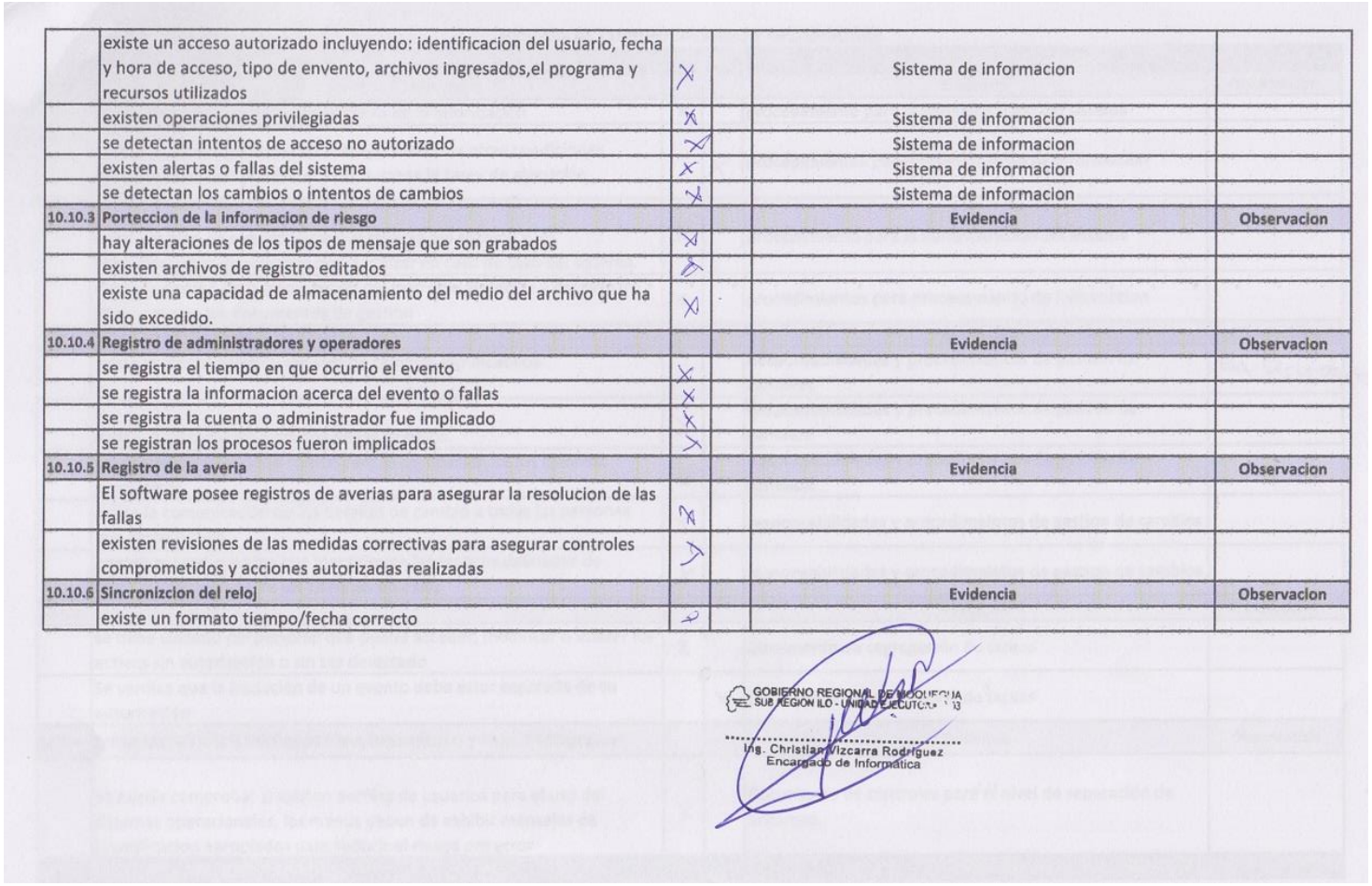
Hoja de evaluación: Gestión de Comunicaciones y operaciones 9



	existe confidecialidad e integridad en cualquier orden de transaccion	X		Política de seguridad de comercio electrónico, Documento especificación del servicio de comercio electrónico.	
	existe un nivel de proteccion requerido para mantener la confidenncialidad e integridad de la informacion de orden	X		Política de seguridad de comercio electrónico	
	se evita la perdida o duplicidad de la informacion	X		Política de seguridad de comercio electrónico	
10.9.2	**Transacciones en línea**			**Evidencia**	**Observacion**
	hay un uso de firmas electronicas por cada una de las partes envueltas en la transaccion	X		Documento de seguridad para transacciones en línea	
	se mantiene la confidencialidad de los detalles de transacciones	X		Documento de seguridad para transacciones en línea	
10.9.3	**informacion publica disponible**			**Evidencia**	**Observacion**
	existe una concordancia de la informacion con la legislacion de proteccion de datos	X		Documentos de procesos formales para la publicación de información	
	el ingreso y procesamiento de la informacion es actualizado a tiempo	X		Políticas de seguridad sobre disponibilidad de información pública	
	la informacionn es protegida durante la recoleccion,procesamiento y almacenamiento.	X		Políticas de seguridad sobre disponibilidad de información pública	
	hay un inaccesible ingreso involuntario a las redes del sistema conectado		X	Políticas de seguridad sobre disponibilidad de información pública	
10.10	Monitoreo	SI	NO		
10.10.1	**Registro de la auditoría**			**Evidencia**	**Observacion**
	se indentifican los usuarios del sistema	X		Sistema de informacion	
	se almacena la fecha y hora de conexión y desconexion	X		Expediente tecnico,Funcionamiento del sistema	
	se identifica el terminal o locacion	X		Funcionamiento del sistema	
	se registra el éxito o fracaso en los intentos de ingreso al sistema	X		expediente tecnico, Funcionamiento del sistema	
	Es posible cambiar la configuracion del sistema	X			
	existen privilegios de acceso en el uso del sistema	X		expedinte tecnico, funcionamiento del sistema	
	se registran los archivos accesados y el tipo de acceso	X			
	existen direcciones de red y protocolos	X			
	exiten alarmas realizadas por el sistema de control de accesos	X			
10.10.2	**Monitoreando el uso del sistema**			**Evidencia**	**Observacion**

Figura 38

Hoja de evaluación: Gestión de Comunicaciones y operaciones 10



	existe un acceso autorizado incluyendo: identificacion del usuario, fecha y hora de acceso, tipo de envento, archivos ingresados,el programa y recursos utilizados	X		Sistema de informacion	
	existen operaciones privilegiadas	X		Sistema de informacion	
	se detectan intentos de acceso no autorizado	X		Sistema de informacion	
	existen alertas o fallas del sistema	X		Sistema de informacion	
	se detectan los cambios o intentos de cambios	X		Sistema de informacion	
10.10.3	**Porteccion de la informacion de riesgo**			**Evidencia**	**Observacion**
	hay alteraciones de los tipos de mensaje que son grabados	X			
	existen archivos de registro editados	X			
	existe una capacidad de almacenamiento del medio del archivo que ha sido excedido.	X			
10.10.4	**Registro de administradores y operadores**			**Evidencia**	**Observacion**
	se registra el tiempo en que ocurrio el evento	X			
	se registra la informacion acerca del evento o fallas	X			
	se registra la cuenta o administrador fue implicado	X			
	se registran los procesos fueron implicados	X			
10.10.5	**Registro de la averia**			**Evidencia**	**Observacion**
	El software posee registros de averias para asegurar la resolucion de las fallas	X			
	existen revisiones de las medidas correctivas para asegurar controles comprometidos y acciones autorizadas realizadas	X			
10.10.6	**Sincronizcion del reloj**			**Evidencia**	**Observacion**
	existe un formato tiempo/fecha correcto	X			

GOBIERNO REGIONAL DE MOQUEGUA
SUB REGION ILO - UNIDAD EJECUTORA

Ing. Christian Vizcarra Rodriguez
Encargado de Informática

Anexo 07

Figura 39

Hoja de evaluación: Control de Acceso 1

CONTROL DE ACCESO					
1	REQUISITOS DE ACCESO	Si	No		
1,1	Politica De Control De Acceso			Evidencia	Observacion
	Existe una politica de acceso que establece reglas y derechos de cada usuario o grupo de usuarios	X		plan de seguridad, (requisitos de seguridad)	
	Existen perfiles de acceso de usuarios estandarizados según las categorías comunes de trabajos	X		Documento P.S.I. (administracion de accesos de usuarios, responsabilidades de usuario: descripción de perfil del usuario (nombre, tipo y numero)	SIAF
	existe administración de los derechos de acceso en un entorno distribuido en red que reconozca todos los tipos disponibles de conexión;	X		Documento P.S.I. (control de acceso a la red: Nombre, tipo y numero)	
	se tiene la segregación de los roles de control de acceso, como el pedido de acceso, autorización de acceso, administración de accesos	X		Documento P.S.I. Administracion de accesos de usuarios(administracion de control de accesos, derechos de acceso de usuarios)	
	se tiene control de retiro de los derechos de acceso	X		Documento de retiro de derechos de acceso	
2	GESTIÓN DE ACCESO DE USUARIOS				
2,1	Registro de usuarios			Evidencia	Observacion
	Existe un identificador único para cada usuario	X		Documento de requisitos y Procedimiento de registro de altas y bajas de usuarios.	
	Se realiza la comprobación de la autorización del usuario por el propietario del servicio para utilizar el sistema.	X		Contratos laborales y de servicio Procedimiento de registro de altas y bajas de usuarios.	
	Existe la petición a los usuarios para que reconozcan con su firma la comprensión de las condiciones de acceso;	X		Contratos laborales y de servicio,Documento de requisitos ,de negocio de la organización,Procedimiento de registro de altas y bajas de usuarios.	
	Existe el mantenimiento de un registro formalizado de todos los autorizados para usar el servicio	X		Contratos laborales y de servicioProcedimiento de registro de altas y bajas de usuarios.	
	Existe un procedimiento que elimina la autorizacion de acceso a los usuarios que dejan la organización o cambien de area	X		Procedimiento de registro de altas y bajas de usuarios.	
	Existe la revisión periódica y eliminación de identificadores y cuentas de usuario redundantes	X		Inventario de Usuarios habilitados y cesados, Procedimiento de registro de altas y bajas de usuarios.	No existe cuenta redundantes
2,2	Gestión De Privilegios			Evidencia	Observacion

T

Figura 40

Hoja de evaluación: Control de Acceso 2

	existen procedimientos para asignar privilegios a los individuos según los principios de "necesidad de su uso" y "caso por caso" y en línea con la política de control de acceso	X		Registro de privilegios asignados,Documento de privilegios disponibles para asignar.	
	existe politicas para mantener un proceso de autorización y un registro de todos los privilegios asignados. No se otorgarán privilegios hasta que el proceso de autorización haya concluido;	X		Registro de privilegios asignados,Documento de privilegios disponibles para asignar.	
2,3	**Gestión De Contraseñas De Usuario**			**Evidencia**	**Observacion**
	Existen compromismo por parte de los usuarios para mantener su contraseña en secreto	X		Compromisos de usuarios a mantener en secreto las contraseñas,	
	Existe un procedimiento que asigne al usuario una contraseña temporal y luego forzasamente esta debe ser cambiada	X		Compromisos de usuarios a mantener en secreto las contraseñas,Registros de contraseñas.	
	Existen metodos que verifiquen la identidad de un usuario para el cambio de contraseña	X		Compromisos de usuarios a mantener en secreto las contraseñas,Registros de falsos negativos y falsos positivos.	
	las contraseñas temporales son únicas para cada individuo y no se obvian	X		Compromisos de usuarios a mantener en secreto las contraseñas,Registros de falsos negativos y falsos positivos.	
	se exige a los usuarios que las contraseñas nunca deben ser almacenadas en sistemas de cómputo sin ser protegidos;	X		Compromisos de usuarios a mantener en secreto las contraseñas,politica de cifrado de contraseñas	
2.4	**Revisión De Los Derechos De Acceso De Los Usuarios**			**Evidencia**	**Observacion**
	Existe un proceso de revision periodica de los derechos de acceso de los usuarios		X	Registro de cambios en cuentas privilegiadas,Derechos de accesos de los usuarios.	
3	RESPONSABILIDADES DE LOS USUARIOS	SI	NO		
3,1	**Uso De Contraseñas**			**Evidencia**	**Observacion**
	Los usuarios siguen buenas practicas de seguridad para la selección y uso de contraseñas	X		Plan de Seguridad	algunos no.
	Se cambian las contraseñas si se tiene algún indicio de su y vulnerabilidad o lo realizan en intervalos de tiempo regulares	X		Acreditacion ante la direccion como empleado.	
	Seleccionan contraseñas de buena calidad, con una longitud mínima caracteres	X		Lineamientos para la construccion, Encriptacion de datos.	
	Incluyen contraseñas en procedimiento automático de conexión, que, las deje almacenadas permanentemente.	X		Ordenadores no autorizados, Bibliotecas, telecentros,etc.	
3,2	**Equipo Informático De Usuario Desatendido**			**Evidencia**	**Observacion**
	Los usuarios y proveedores de servicios conocen los requisitos de seguridad y los procedimiento para proteger los equipos desatendidos	X		Servidores de archivos o estacion de trabajo	

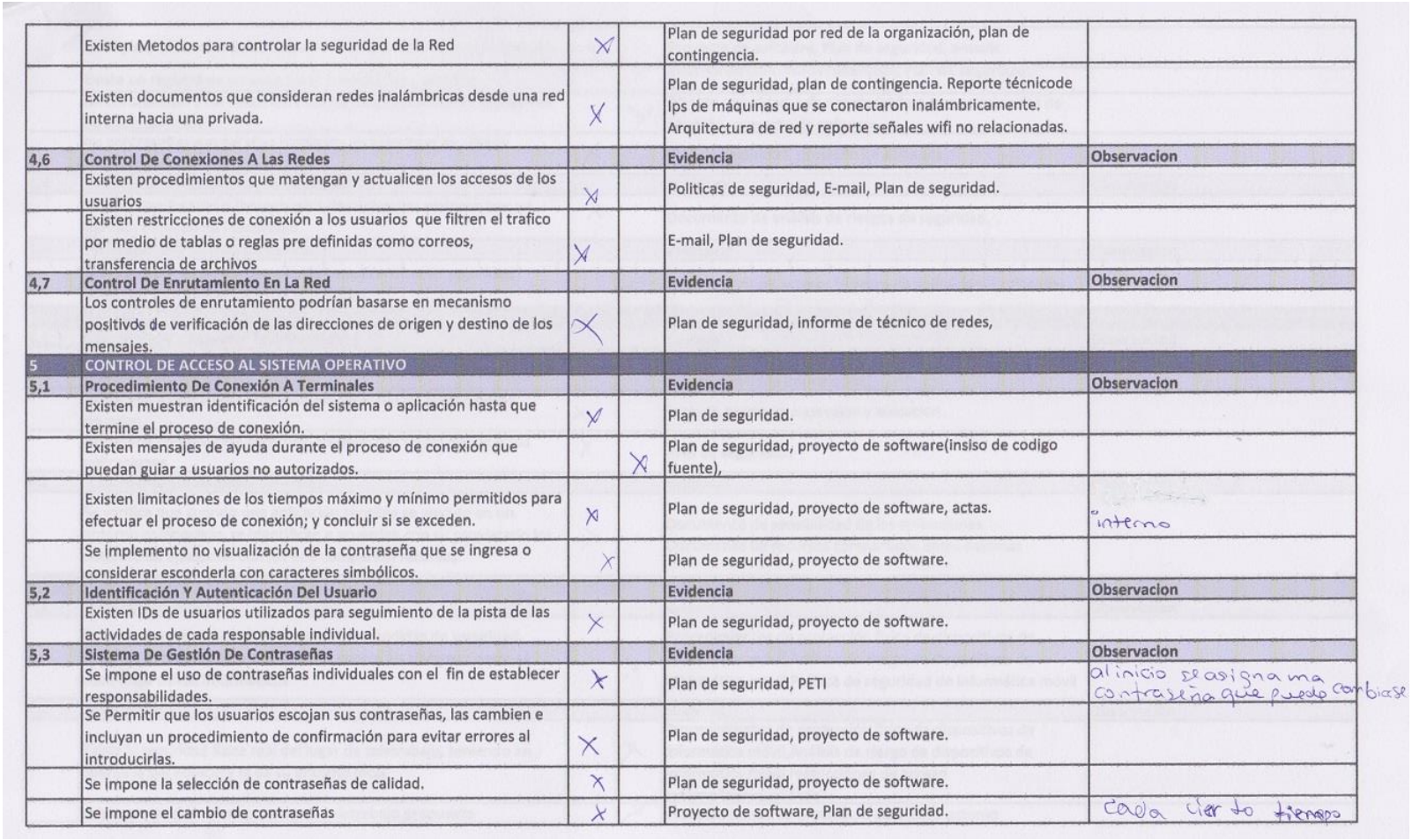
Figura 41

Hoja de evaluación: Control de Acceso 3

	Los usuarios tienen buenas practicas para los equipos desatendidos como: cancelar las sesiones al irse, desconectar los equipos, bloquear el equipo cuando no este en uso		X	Plan de seguridad.	
3,3	**Política De Pantalla Y Escritorio Limpio**			**Evidencia**	**Observacion**
	Existen una medida de proteccion de la información critica o sensible del negocio cuando no sea requerido, especialmente cuando la oficina este vacía.	X		Documentos, correos.	
	Existen una proteccion de los puntos salientes o entrantes de correo y los faxes que estan desatendidos.	X		Email, documentos	
	Existen una prevencion del uso no autorizado de fotocopiadoras y otras tecnologías de reproducción como scanner o cámaras digitales.	X		Plan de seguridad, medida de seguridad.	
4	CONTROL DE ACCESO A LA RED				
4,1	**Política De Uso De Los Servicios De La Red**			**Evidencia**	**Observacion**
	Existen procedimientos de acceso directo a los servicios solamente para los que esta autorizado el usuario en forma especifica	X		Plan de seguridad, plan de redes, PETI.	
4,2	**Autentificación De Usuario Para Conexiones Externas**			**Evidencia**	**Observacion**
	Existen procedimientos que aseguren la autentificacion de usuarios remotos como tecnicas de criptografia. Con el fin de asegurar las fuentes de conexiones	X		Plan de seguridad, firma digital, certificado digital. Cedulas de control de conexión, Sutsourcing	
	Existen controles adicionales de autentificación e implementados para el control de acceso de redes inalámbricas.	X		Plan de seguridad, manual de moden, imágenes de configuracion para esta seguridad, informes de implementacion.	
4,3	**Identificación De Los Servicios De Redes**			**Evidencia**	**Observacion**
	Hay identificadores de equipos que son utilizados para que comunicaciones sean iniciadas desde un local y equipos especifico. Indicador de equipos autorizados.	X		Plan de seguridad, certificado digital, documento de adquisición de software de firmas digitales.	Posee conflicto de autentificacion en los equipos
4,4	**Diagnósticos Remotos Y Configuración De Puertos.**			**Evidencia**	**Observacion**
	Existen controles potenciales para el acceso de diagnostico y configuración de puertos que incluyen el uso de un cierre de llave y de procedimientos de apoyo para controlar el acceso físico al puerto.	X		Plan de seguridad(informe técnico de configuración de puertos)	
	Existen puertos, servicios e instalaciones similares instaladas en una computadora o instalación de computo no son requeridas específicamente para la funcionabilidad del negocio, que hayan sido inhabilitado o removido.		X	Memorandum, reporte técnico de requerimientos de hardware software que es usado y no usado	
4,5	**Segregación En Las Redes**			**Evidencia**	**Observacion**

Figura 42

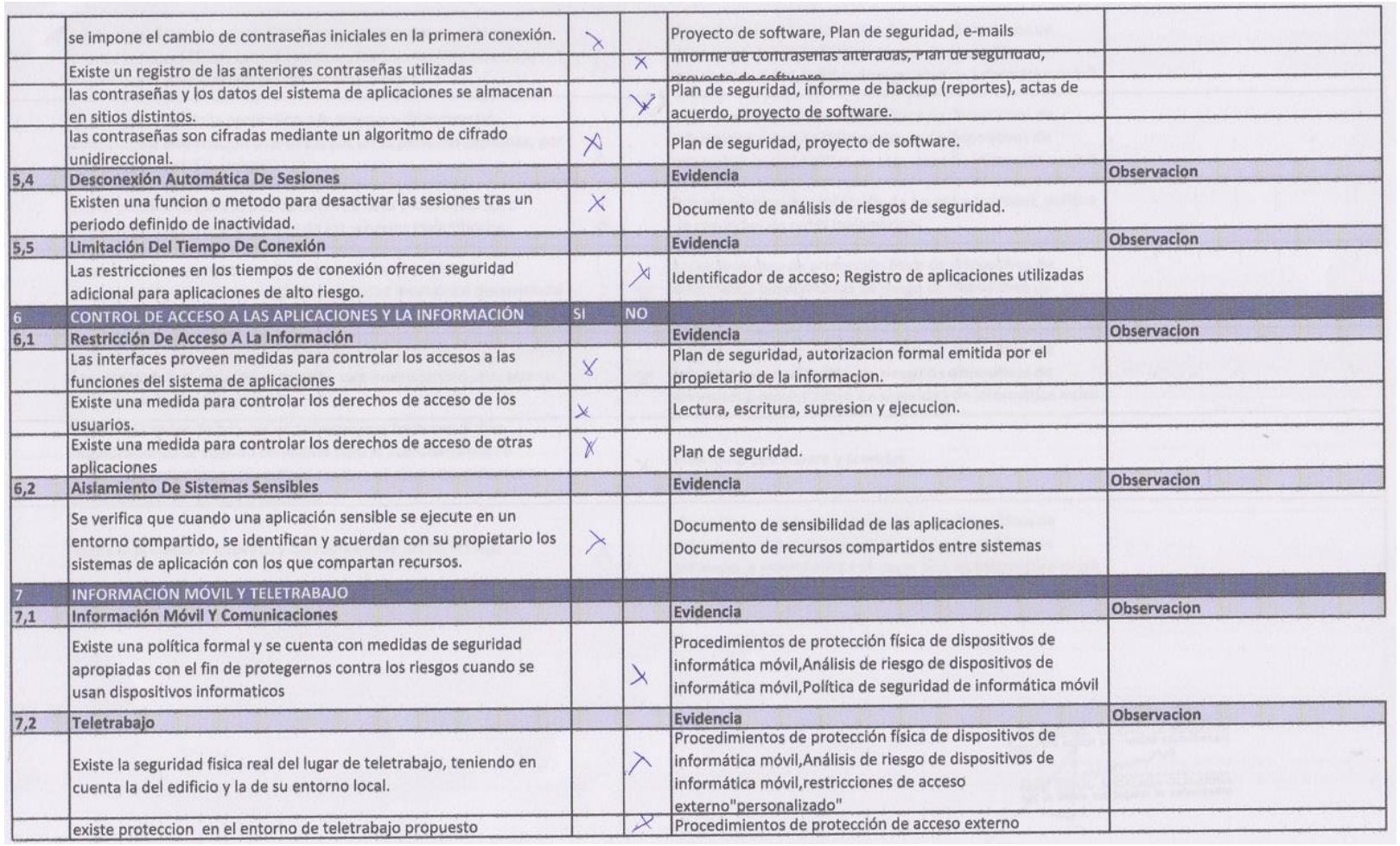
Hoja de evaluación: Control de Acceso 4



	Existen Metodos para controlar la seguridad de la Red	X		Plan de seguridad por red de la organización, plan de contingencia.	
	Existen documentos que consideran redes inalámbricas desde una red interna hacia una privada.	X		Plan de seguridad, plan de contingencia. Reporte técnicode Ips de máquinas que se conectaron inalámbricamente. Arquitectura de red y reporte señales wifi no relacionadas.	
4,6	**Control De Conexiones A Las Redes**			**Evidencia**	**Observacion**
	Existen procedimientos que matengan y actualicen los accesos de los usuarios	X		Politicas de seguridad, E-mail, Plan de seguridad.	
	Existen restricciones de conexión a los usuarios que filtren el trafico por medio de tablas o reglas pre definidas como correos, transferencia de archivos	X		E-mail, Plan de seguridad.	
4,7	**Control De Enrutamiento En La Red**			**Evidencia**	**Observacion**
	Los controles de enrutamiento podrían basarse en mecanismo positivos de verificación de las direcciones de origen y destino de los mensajes.	X		Plan de seguridad, informe de técnico de redes,	
5	**CONTROL DE ACCESO AL SISTEMA OPERATIVO**				
5,1	**Procedimiento De Conexión A Terminales**			**Evidencia**	**Observacion**
	Existen muestran identificación del sistema o aplicación hasta que termine el proceso de conexión.	X		Plan de seguridad.	
	Existen mensajes de ayuda durante el proceso de conexión que puedan guiar a usuarios no autorizados.		X	Plan de seguridad, proyecto de software(insiso de codigo fuente),	
	Existen limitaciones de los tiempos máximo y mínimo permitidos para efectuar el proceso de conexión; y concluir si se exceden.	X		Plan de seguridad, proyecto de software, actas.	"interno
	Se implemento no visualización de la contraseña que se ingresa o considerar esconderla con caracteres simbólicos.	X		Plan de seguridad, proyecto de software.	
5,2	**Identificación Y Autenticación Del Usuario**			**Evidencia**	**Observacion**
	Existen IDs de usuarios utilizados para seguimiento de la pista de las actividades de cada responsable individual.	X		Plan de seguridad, proyecto de software.	
5,3	**Sistema De Gestión De Contraseñas**			**Evidencia**	**Observacion**
	Se impone el uso de contraseñas individuales con el fin de establecer responsabilidades.	X		Plan de seguridad, PETI	al inicio se asigna una contraseña que puede cambiarse
	Se Permitir que los usuarios escojan sus contraseñas, las cambien e incluyan un procedimiento de confirmación para evitar errores al introducirlas.	X		Plan de seguridad, proyecto de software.	
	Se impone la selección de contraseñas de calidad.	X		Plan de seguridad, proyecto de software.	
	Se impone el cambio de contraseñas	X		Proyecto de software, Plan de seguridad.	Cada cierto tiempo

Figura 43

Hoja de evaluación: Control de Acceso 5



	se impone el cambio de contraseñas iniciales en la primera conexión.	X		Proyecto de software, Plan de seguridad, e-mails	
	Existe un registro de las anteriores contraseñas utilizadas		X	Informe de contraseñas alteradas, Plan de seguridad, proyecto de software	
	las contraseñas y los datos del sistema de aplicaciones se almacenan en sitios distintos.		X	Plan de seguridad, informe de backup (reportes), actas de acuerdo, proyecto de software.	
	las contraseñas son cifradas mediante un algoritmo de cifrado unidireccional.	X		Plan de seguridad, proyecto de software.	
5,4	**Desconexión Automática De Sesiones**			**Evidencia**	**Observacion**
	Existen una funcion o metodo para desactivar las sesiones tras un periodo definido de inactividad.	X		Documento de análisis de riesgos de seguridad.	
5,5	**Limitación Del Tiempo De Conexión**			**Evidencia**	**Observacion**
	Las restricciones en los tiempos de conexión ofrecen seguridad adicional para aplicaciones de alto riesgo.		X	Identificador de acceso; Registro de aplicaciones utilizadas	
6	CONTROL DE ACCESO A LAS APLICACIONES Y LA INFORMACIÓN	SI	NO		
6,1	**Restricción De Acceso A La Información**			**Evidencia**	**Observacion**
	Las interfaces proveen medidas para controlar los accesos a las funciones del sistema de aplicaciones	X		Plan de seguridad, autorizacion formal emitida por el propietario de la informacion.	
	Existe una medida para controlar los derechos de acceso de los usuarios.	X		Lectura, escritura, supresion y ejecucion.	
	Existe una medida para controlar los derechos de acceso de otras aplicaciones	X		Plan de seguridad.	
6,2	**Aislamiento De Sistemas Sensibles**			**Evidencia**	**Observacion**
	Se verifica que cuando una aplicación sensible se ejecute en un entorno compartido, se identifican y acuerdan con su propietario los sistemas de aplicación con los que compartan recursos.	X		Documento de sensibilidad de las aplicaciones. Documento de recursos compartidos entre sistemas	
7	INFORMACIÓN MÓVIL Y TELETRABAJO				
7,1	**Información Móvil Y Comunicaciones**			**Evidencia**	**Observacion**
	Existe una política formal y se cuenta con medidas de seguridad apropiadas con el fin de protegernos contra los riesgos cuando se usan dispositivos informaticos		X	Procedimientos de protección física de dispositivos de informática móvil,Análisis de riesgo de dispositivos de informática móvil,Política de seguridad de informática móvil	
7,2	**Teletrabajo**			**Evidencia**	**Observacion**
	Existe la seguridad fisica real del lugar de teletrabajo, teniendo en cuenta la del edificio y la de su entorno local.		X	Procedimientos de protección física de dispositivos de informática móvil,Análisis de riesgo de dispositivos de informática móvil,restricciones de acceso externo"personalizado"	
	existe proteccion en el entorno de teletrabajo propuesto		X	Procedimientos de protección de acceso externo	

Figura 44

Hoja de evaluación: Control de Acceso 6

	Existen requisitos de seguridad de las comunicaciones, teniendo en cuenta la nesecidad de acceso remoto a los sitemas internos de la organizacion y de la criticidad del sistema interno	X		Procedimientos de protección física de dispositivos de informática móvil,Análisis de riesgo de dispositivos de informática móvil,Política de seguridad de informática móvil	
	se a implementado la proteccion a la amenaza de acceso no autorizado a informacion y recursos por otras personas proximas, por ejemplo, la familia o amigos	X		Procedimientos de protección física de dispositivos de informática móvil,Análisis de riesgo de dispositivos de informática móvil,Política de seguridad de informática móvil	
	Existe proteccion para el uso de redes de casa y los requisitos o restricciones de la configuracion de los servicios inalambricos	X		Procedimientos de protección de acceso a las redes ,politica de seguridad de redes inalambricas	
	existe politicas y procemientos para prevenir las disputas concernientes a los derechos de la propiedad intelectual desarrollada en equipos privados propios		X	Procedimientos de protección física de dispositivos de informática móvil,Análisis de riesgo de dispositivos de informática móvil,Política de seguridad de informática móvil	
	existe proteccion de acceso a un equipo privado propio (para verificar la seguridad de la maquina o durante una investigacion), que puede ser prevenido por la legislacion		X	Procedimientos de protección física de dispositivos de informática móvil,Análisis de riesgo de dispositivos de informática móvil,Política de seguridad de informática móvil	
	Existen acuerdos de licencia de software que hara que dichas organizaciones se vuelvan confiables para el licenciamiento de software de clientes en las estaciones de trabajo pertenecientes a empleados, contratistas o terceros		X	inventario desoftware y licencias	
	existe la proteccion antivirus y los requerimientos de firewall	X		Procedimientos de protección física de dispositivos de informática móvil,Análisis de riesgo de dispositivos de informática móvil,Política de seguridad de informática móvil	

GOBIERNO REGIONAL DE MOQUEGUA
SUB REGIÓN ILO - UNIDAD EJECUTORA-003
Abog. EMILIO ENCALADA OLAVARRIA
Jefe de Oficina Sub Regional de Administración

Anexo 08

Figura 45

Hoja de evaluación: Adquisición, desarrollo y mantenimiento de sistemas 1

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS					
1	Requisitos de seguridad de los sistemas	Si	No		
1.1	**Análisis y especificación de los requisitos de seguridad**			**Evidencia**	**Observacion**
	Se comprueba que se consideren los controles automatizados a ser incorporados en el sistema y la necesidad de controles manuales de apoyo. Lo mismo cuando se evalua, desarrolla o compra paquetes de software	X		Documento de evaluación de productos de seguridad de TI Requisitos de seguridad de la organización Documento de valorización de activos de información	
	Los requisitos y controles de seguridad reflejan el valor de los activos de información implicados y el posible daño a la organización que resultaría de fallos o ausencia de seguridad.	X		Documento de evaluación de productos de seguridad de TI Requisitos de seguridad de la organización Documento de valorización de activos de información	
	Los requisitos del sistema para la seguridad de información y procesos para implementar la seguridad son integrados en las etapas iniciales de los proyectos de sistema de información	X		Documento de evaluación de productos de seguridad de TI Requisitos de seguridad de la organización Documento de valorización de activos de información	
	Si los productos son comprados, se realiza una prueba formal y un proceso de adquisición. Los contratos con el proveedor deben indicar los requisitos de seguridad.	X		Documento de evaluación de productos de seguridad de TI Requisitos de seguridad de la organización Documento de valorización de activos de información	
2	Seguridad de las aplicaciones del sistema				
2.1	**Validación de los datos de entrada**			**Evidencia**	**Observacion**
	Se comprueba que se aplican verificaciones a la entrada de las transacciones, de los datos de referencia y de las tablas de parámetros.	X		-	
	Se controla la entrada duplicada, valores fuera de rango, caracteres invalidos, datos incompletos, datos que excedan limites de volumen, datos de controles inconsistentes.	X		-	
	Se revisa periodicamente el contenido de los campos clave o de los archivos de datos para confirmar su validez e integridad.	X		-	
	Se inspeccionan los documentos físicos de entrada para ver si hay cambios no autorizados a los datos de entrada	X		-	
	Existen procedimientos para responder a los errores de validación	X		-	
	Existen procedimientos para comprobar la integridad de los datos de entrada.	X		-	
2.2	**Control del proceso interno**			**Evidencia**	**Observacion**
	Existen restricciones que minimicen el riesgo de los fallos del proceso con pérdidas de integridad.	X		Listas de verificación. Documentación de actividades y resultados	

Figura 46

Hoja de evaluación: Adquisición, desarrollo y mantenimiento de sistemas 2

	Existe una lista de verificación apropiada donde se tiene las actividades documentadas y los resultados seguros.		X	Listas de verificación. Documentación de actividades y resultados	
2.3	**Integridad de mensajes**			**Evidencia**	**Observacion**
	Se realizó una evaluación de riesgos para determinar si la integridad de los mensajes es requerida y que se ha identificado el método mas apropiado para su implementación.		X	Documento de implantación para autenticación	
2.4	**Validación de los datos de salida**			**Evidencia**	**Observacion**
	Existe la validacaión de los datos de salida.	X		Documento de validación, verificación y prueba de los sistemas y aplicaciones	
3	Controles criptográficos				
3.1	**Política de uso de los controles criptográficos**			**Evidencia**	**Observacion**
	Existe un enfoque de gestión del uso de las medidas criptográficas.	X		Documento de requisitos de seguridad de la organización Procedimientos de uso de información cifrada.	
	Existe una política basada en la evaluación de riesgos.		X	Documento de requisitos de seguridad de la organización Documento de roles y responsabilidades Documento de Evaluación de riesgos	
	Se utiliza cifrado para la protección de información sensible transportada en dispositivos móviles o removibles y en las líneas de comunicación.	X		Procedimientos de uso de información cifrada. Documento de Evaluación de riesgos	
	Existe un enfoque de gestión de claves, que incluyen métodos para tratar la recuperación de la información cifrada.		X	Documento de requisitos de seguridad de la organización Documento de roles y responsabilidades Procedimientos de uso de información cifrada.	
	Existen roles y responsabilidades de la implementación de la política y la gestión de claves-		X	Documento de requisitos de seguridad de la organización Documento de roles y responsabilidades	
	Existen estándares para ser adoptados en una efectiva implementación a través de la organización		X	Documento de requisitos de seguridad de la organización Documento de roles y responsabilidades	
	Existen normas para utilizar información cifrada en controles que confíen en la inspección de contenido.		X	Procedimientos de uso de información cifrada. Documento de Evaluación de riesgos	
	Se utilizan controles criptográficos para alcanzar diferentes objetivos de seguridad.	X		Procedimientos de uso de información cifrada. Documento de Evaluación de riesgos	
3.2	**Gestión de claves**			**Evidencia**	**Observacion**
	Existe un sistema de gestión de claves (criptograficos, para generar,distribuir, almacenar, revocar, recuperar, destruir y/o auditar claves).		X	Documentos de acuerdos de nivel de servicio. Contratos con proveedores de servicios criptográficos	
	Se comprueba la autenticidad de la claves públicas mediante una autoridad certificadora.		X	Documentos de acuerdos de nivel de servicio. Contratos con proveedores de servicios criptográficos	

Figura 47

Hoja de evaluación: Adquisición, desarrollo y mantenimiento de sistemas 3

4	Seguridad de los archivos del sistema				
4.1	**Control del software en producción.**			**Evidencia**	**Observacion**
	Sólo el administrador capacitado, previa autorización de gerencia, realiza la actualización de las librerías de programas operativos	X		Documento de estrategia de restauración.	
	Se verifica que no se implante código en un sistema operativo mientras no se tenga evidencia del éxito de las pruebas, la aceptación del usuario y la actualización de las librerías de programas fuentes.	X		Documento de estrategia de restauración.	
	Existe una estrategia de restauración no actualizada antes de que se implementen los cambios	X		Informes de auditoria Documento de estrategia de restauración.	
	Se archivan las versiones antiguas de software junto con toda la información requerida en caso de auditorias.	X		Informes de auditoria Documento de estrategia de restauración.	
4.2	**Protección de los datos de prueba del sistema**			**Evidencia**	**Observacion**
	Los procedimientos de control de acceso que se consideran para las aplicaciones del sistema operacional son utilizados también en los sistemas de aplicaciones en prueba.	X		Documentos de procedimientos de control de acceso a aplicaciones del sistema operacional	
	Se autoriza por separado cada vez que se copia información operativa a un sistema de aplicación o en prueba	X		Registros de copiado y uso de información operativa Documentos de procedimientos de control de acceso a aplicaciones del sistema operacional	
	Se borra la información operativa de la aplicación del sistema en prueba en cuanto ésta se complete	X		Registros de copiado y uso de información operativa	
	Se registra la copia y uso de la información operativa a efectos de seguimiento para auditoria		X	Registros de copiado y uso de información operativa Documentos de procedimientos de control de acceso a aplicaciones del sistema operacional	
4.3	**Control de acceso a los códigos de programas fuente**			**Evidencia**	**Observacion**
	Las librerías de programas fuentes tiene acceso restringido	X		Documento de responsabilidades y roles de seguridad Actas de uso de códigos y librerías de programas fuente.	
	Existen procedimientos establecidos para maniobrar el código y librería de programas fuente.		X	Documento de responsabilidades y roles de seguridad Actas de uso de códigos y librerías de programas fuente.	
	Existe restricciones para personal de apoyo informático en el acceso a las librería de programas fuentes.	X		Documento de responsabilidades y roles de seguridad Actas de uso de códigos y librerías de programas fuente.	
	La actualización de librerías de programas y la entrega de programas a los programadores sólo se realiza por el responsable con autorización del gerente de soporte informático para la aplicación	X		Registros de auditoria de accesos a librerías de programas fuentes Documento de responsabilidades y roles de seguridad Actas de uso de códigos y librerías de programas fuente. Procedimientos de control de cambios	
	Los listados de programas se mantienen en un entorno seguro	X		Documento de responsabilidades y roles de seguridad	

Figura 48

Hoja de evaluación: Adquisición, desarrollo y mantenimiento de sistemas 4

	Se mantiene un registro de auditoria de todos los accesos a las librerías de programas fuentes.		X	Registros de auditoria de accesos a librerías de programas fuentes Documento de responsabilidades y roles de seguridad	
	El mantenimiento y copia de librerías de programas fuente esta sujeto a procedimientos estrictos de control de cambios		X	Actas de uso de códigos y librerías de programas fuente. Procedimientos de control de cambios	
5	**Seguridad en los procesos de desarrollo y soporte**				
5.1	**Procedimientos de control de cambios**			**Evidencia**	**Observacion**
	Existe un proceso de control de cambios incluye una evaluación de riesgos, un análisis de los impactos de los cambios y una especificación de los controles de seguridad necesarios.		X	Documento de gestión de cambios	
	La aplicación y sus procedimientos de control de cambios estan integrados siempre que sea posible.		X	Documento de gestión de cambios	
5.2	**Revisión técnica de los cambios en el sistema operativo**			**Evidencia**	**Observacion**
	Existe una revisión de los procedimientos de control de la aplicación y de la integridad.	X		Documento del proceso de cambios en el sistema operativo Procedimientos de control de la aplicación y de la integridad	
	Cubre la garantía de que la modificación de los cambios del sistema operativos se realiza a tiempo para que puedan hacerse las revisiones apropiadas antes de su implantación		X	Documento del proceso de cambios en el sistema operativo Procedimientos de control de la aplicación y de la integridad	
	cubre la garantía de que se realizan los cambios apropiados en los planes de continuidad del negocio		X	Documento del proceso de cambios en el sistema operativo Procedimientos de control de la aplicación y de la integridad	
5.3	**Restricciones en los cambios a los paquetes de software**			**Evidencia**	**Observacion**
	Se tomó en cuenta el riesgo de debilitamiento de las medidas de control incorporadas y sus procesos de integridad	X		Documento de análisis de impacto por el cambio del paquete del software Procedimientos de control de la aplicación y de la integridad	
	Se tomó en cuenta la obtención del consentimiento del vendedor		X	Procedimientos de control de la aplicación y de la integridad	
	Se tomó en cuenta la posibilidad de obtener los camabios requeridos como actualizaciones normales del programa del vendedor	X		Documento de análisis de impacto por el cambio del paquete del software	

Figura 49

Hoja de evaluación: Adquisición, desarrollo y mantenimiento de sistemas 5

	Se tomó en cuenta el impacto causado si la organización adquiere la responsabilidad del mantenimiento futuro del software		X	Documento de análisis de impacto por el cambio del paquete del software Procedimientos de control de la aplicación y de la integridad	
5.4	**Fuga de información**			**Evidencia**	**Observacion**
	Se limita el riesgo de fuga de información	X		Documento de riesgos de fuga de información Documento de controles para la fuga de información	
5.5	**Desarrollo externo del software**			**Evidencia**	**Observacion**
	El desarrollo de lsoftware es supervisado y monitoreado por la organización y se consideran distintos acuerdos de propiedad.	X		Documento de procedimientos para el desarrollo externo del software Acuerdos bajo licencia Contratos con entidad desarrolladora del software Documento de pruebas del software	
6	**Gestión de la vulnerabilidad técnica**				
6.1	**Control de las vulnerabilidades técnicas.**			**Evidencia**	**Observacion**
	Existen roles establecidos y responsabilidades asociadas con la gestion de vulnerabilidades tecnicas.		X	-	
	Existen recursos de información utilizados para identificar las vulnerabilidades tecnicas relevantes.	X		-	
	Existe definida una linea de tiempo para reaccionar ante notificaciones de vulnerabilidades técnicas potenciales y relevantes.	X		-	
	Se identifican los riesgos asociados (a las vulnerabilidades técnicas) y las acciones a ser tomadas en cuenta.	X		-	

GOBIERNO REGIONAL DE MOQUEGUA
SUB REGION II.O | UNIDAD EJECUTORA - 003

Ing. Christian Vizcarra Rodríguez
Encargado de Informática

Anexo 09

Acta De Requerimientos SIAF

Tabla 1

Cuadro de requerimientos funcionales SIAF

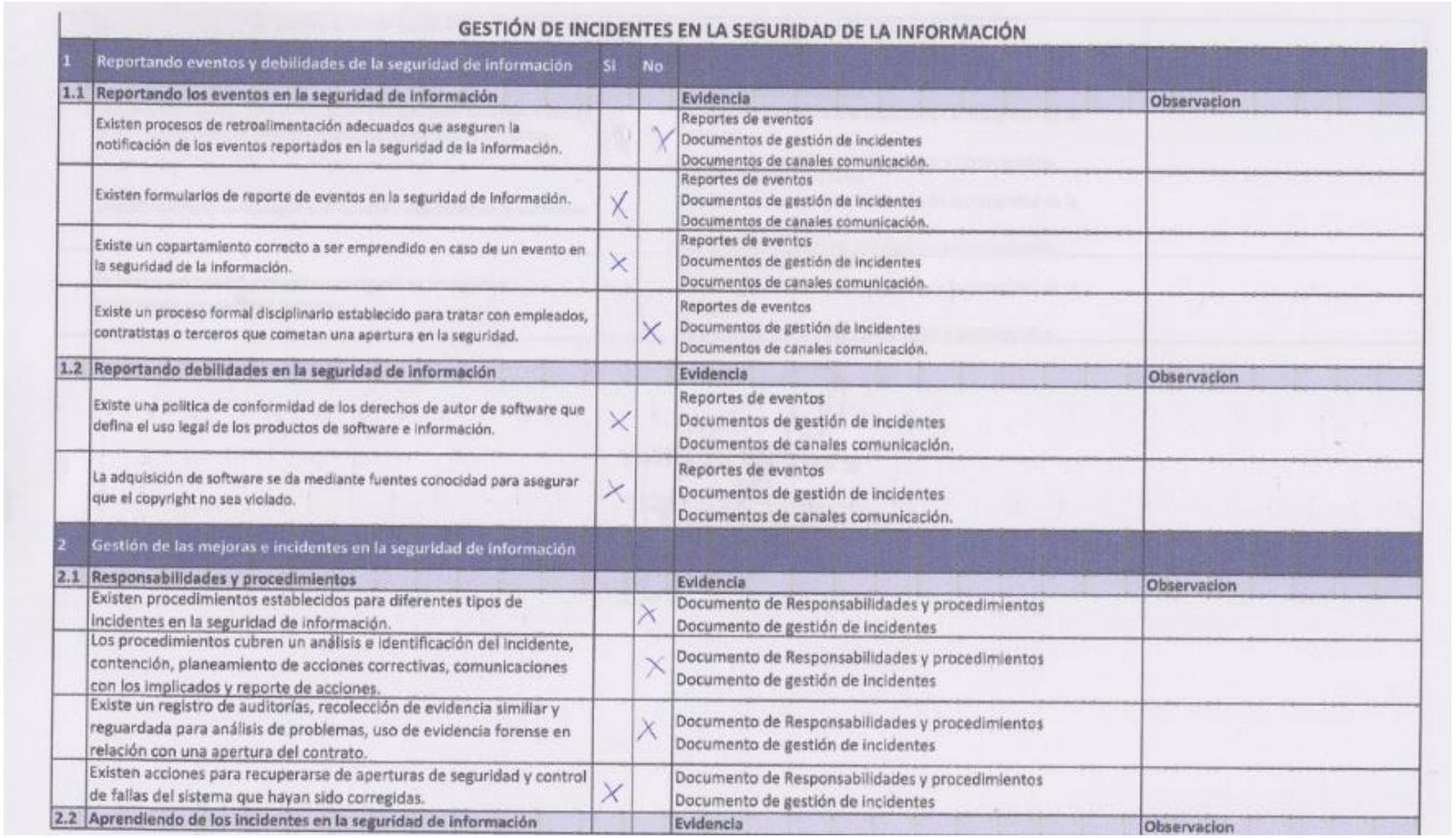
CUADRO DE REQUERIMIENTOS FUNCIONALES		
REQUERIMIENTOS	**CUMPLE**	
	SI	**NO**
Requerimientos generales del Acceso al Sistema.		
Abrir el Sistema	X	
Ingresar cuenta de usuario	X	
Ingresa Contraseña	X	
Verifica la existe del usuario	X	
Muestra menú para elección de módulos	X	
Muestra pantalla principal del módulo elegido		
Requerimientos generales de Registro.		
Control de valores o caracteres inválidos	X	
Verificar existencia del registro	X	
Si no existe se registra	X	
Si existe se puede modificar	X	
Si se comprueba que no existe, se realiza el registro	X	
Se puede anular registro	X	
Cuenta con ayuda	X	
Cuenta con botón de deshacer	X	
Cuenta con botón para guardar	X	
Cuenta con botón para salir	X	
Cuenta con lista de opciones con códigos numéricos	X	
Tiene un formato de fecha establecido	X	
Cuenta con distintos formatos de moneda	X	
Cuenta con mensajes emergentes	X	
Muestra mensaje al ingresar fecha errónea	X	
Muestra mensaje al no ingresar algún dato	X	
Registro de Fase Compromiso	X	
Registro de Fase Devengado	X	

Registro de Fase Girado	X
Registro de Fase Pagado	X
Contabiliza de Fase Compromiso	X
Contabiliza de Fase Devengado	X
Contabiliza de Fase Devengado	X
Contabiliza de Fase Devengado	X
Contabiliza Documentos Entregados	X
Requerimientos generales de la Gestión de Informes	
Balance General	X
Estado de Gestión	X
Estado de ejecución del presupuesto de ingresos y gastos	X
Anexos financieros	X
Estados Presupuestarios	X

Anexo 10

Figura 50

Hoja de evaluación: Gestión de incidentes en la seguridad de la información 1



GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN					
1	Reportando eventos y debilidades de la seguridad de información	Si	No		
1.1	**Reportando los eventos en la seguridad de información**			Evidencia	Observacion
	Existen procesos de retroalimentación adecuados que aseguren la notificación de los eventos reportados en la seguridad de la información.		X	Reportes de eventos Documentos de gestión de incidentes Documentos de canales comunicación.	
	Existen formularios de reporte de eventos en la seguridad de información.	X		Reportes de eventos Documentos de gestión de incidentes Documentos de canales comunicación.	
	Existe un copartamiento correcto a ser emprendido en caso de un evento en la seguridad de la información.	X		Reportes de eventos Documentos de gestión de incidentes Documentos de canales comunicación.	
	Existe un proceso formal disciplinario establecido para tratar con empleados, contratistas o terceros que cometan una apertura en la seguridad.		X	Reportes de eventos Documentos de gestión de incidentes Documentos de canales comunicación.	
1.2	**Reportando debilidades en la seguridad de información**			Evidencia	Observacion
	Existe una política de conformidad de los derechos de autor de software que defina el uso legal de los productos de software e información.	X		Reportes de eventos Documentos de gestión de incidentes Documentos de canales comunicación.	
	La adquisición de software se da mediante fuentes conocidad para asegurar que el copyright no sea violado.	X		Reportes de eventos Documentos de gestión de incidentes Documentos de canales comunicación.	
2	Gestión de las mejoras e incidentes en la seguridad de información				
2.1	**Responsabilidades y procedimientos**			Evidencia	Observacion
	Existen procedimientos establecidos para diferentes tipos de incidentes en la seguridad de información.		X	Documento de Responsabilidades y procedimientos Documento de gestión de incidentes	
	Los procedimientos cubren un análisis e identificación del incidente, contención, planeamiento de acciones correctivas, comunicaciones con los implicados y reporte de acciones.		X	Documento de Responsabilidades y procedimientos Documento de gestión de incidentes	
	Existe un registro de auditorías, recolección de evidencia similiar y reguardada para análisis de problemas, uso de evidencia forense en relación con una apertura del contrato.		X	Documento de Responsabilidades y procedimientos Documento de gestión de incidentes	
	Existen acciones para recuperarse de aperturas de seguridad y control de fallas del sistema que hayan sido corregidas.	X		Documento de Responsabilidades y procedimientos Documento de gestión de incidentes	
2.2	**Aprendiendo de los incidentes en la seguridad de información**			Evidencia	Observacion

Figura 51

Hoja de evaluación: Gestión de incidentes en la seguridad de la información 2

	Existe un mecanismo de identificación de incidentes frecuentes o de gran impacto	X		Documento de gestión de incidentes Registro de incidentes de la organización	
2.3	**Recolección de evidencia**			**Evidencia**	**Observacion**
	Los sistemas de información cumplen con cualquier estandar o codigo publicado de práctica para la producción de evidencia admisible.	X		Documento de evidencias Procedimientos para la protección de la integridad de la evidencia Documento legislativos, regulatorios y contractuales.	
	Existen controles para asegurar la calidad y seguridad de la evidencia.	X		Documento de evidencias Procedimientos para la protección de la integridad de la evidencia Documento legislativos, regulatorios y contractuales.	
	La integridad de todo material en evidencia es protegida y supervisada por personal confiable.	X		Documento de evidencias Procedimientos para la protección de la integridad de la evidencia Documento legislativos, regulatorios y contractuales.	

GOBIERNO REGIONAL DE MOQUEGUA
SUB REGION ILO - UNIDAD EJECUTORA - 002

Ing. Christian Vizcarra Rodríguez
Encargado de Informática

Anexo 11

Figura 52

Hoja de evaluación: Cumplimiento 1

CUMPLIMIENTO					
1	Cumplimiento con los requisitos legales	Si	No		
1.1	**Identificación de la legislación aplicable**			**Evidencia**	**Observacion**
	Existen controles, medidas y responsabilidades definidos y documentados para cumplir los requisitos legales en el Perú.	X		Documento de requisitos legales, regulares y contractuales para cada sistema de información.	
1.2	**Derechos de propiedad intelectual**			**Evidencia**	**Observacion**
	Existe una política de conformidad de los derechos de autor del software que defina el uso legal de los productos de software e información.	X		Términos y condiciones del software (Licencia) Documento de requisitos legislativos, regulatorios y contractuales.	
	El software es adquirido mediante fuentes conocidas para asegurar que el copyright no sea violado	X		Términos y condiciones del software (Licencia) Documento de requisitos legislativos, regulatorios y contractuales. Documentación de propiedad intelectual.	
	Existe concientización sobre los derechos de autor del software y políticas de adquisiciones.	X		Términos y condiciones del software (Licencia) Documento de requisitos legislativos, regulatorios y contractuales. Documentación de propiedad intelectual	
	Los activos están registrados apropiadamente.	X		Términos y condiciones del software (Licencia) Documento de requisitos legislativos, regulatorios y contractuales.	
	Existen documentos que acreditan la propiedad de licencias, material original, manuales,etc.	X		Términos y condiciones del software (Licencia) Documentación de propiedad intelectual	
	Existe una política de conformidad de los derechos de autor del software que defina el uso legal de los productos de software e información.	X		Términos y condiciones del software (Licencia) Documento de requisitos legislativos, regulatorios y contractuales.	
	Existe instalación sólo de software autorizado y de productos bajo licencia.		X	Términos y condiciones del software (Licencia)	No se cuenta con licencia de algunos programas
	Existe una política establecida de mantenimiento de las condiciones adecuadas de la licencia.		X	Términos y condiciones del software (Licencia) Documento de requisitos legislativos, regulatorios y contractuales.	
	Existe una política establecida de eliminación de software o de su transferencia a terceros.		X	Términos y condiciones del software (Licencia) Documento de requisitos legislativos, regulatorios y contractuales.	
	Existe un uso de herramientas adecuadas de auditoría.		X	Términos y condiciones del software (Licencia) Documento de requisitos legislativos, regulatorios y contractuales.	
	Existe un cumplimiento de los términos y condiciones de uso del software y de la información obtenida de redes públicas.	X		Términos y condiciones del software (Licencia) Documento de requisitos legislativos, regulatorios y contractuales.	

Figura 53

Hoja de evaluación: Cumplimiento 2

	Se cumple con las prohibiciones por la ley de copyright (duplicado, convertido en otro formato o extracción).	X		Términos y condiciones del software (Licencia) Documento de requisitos legislativos, regulatorios y contractuales. Documentación de propiedad intelectual (que incluyen al software o copyright del documento, derechos de diseño, marca registrada, patente y fuentes de licencia de código)	
1.3	**Salvaguarda de los registros de la organización**			**Evidencia**	**Observacion**
	Existen guías publicadas sobre la retención, almacenamiento, tratamiento y eliminación de regristro y la información,.	X		Registros contables, de base de datos, de transacciones, de auditoria. Documento de requisitos legislativos, regulatorios y contractuales.	
	Existe un calendario de retenciones que identifica los periodos para cada tipo esencial de registros.		X	Registros contables, de base de datos, de transacciones, de auditoria.	
	Existe un inventario de las fuentes de información clave.		X	Registros contables, de base de datos, de transacciones, de auditoria. Documento de requisitos legislativos, regulatorios y contractuales.	
	Existe una implementación de controles y medidas apropiadas para la protección de los registros y la información esencial contra su pérdida, destrucción o falsificación.		X	Registros contables, de base de datos, de transacciones, de auditoria. Documento de requisitos legislativos, regulatorios y contractuales.	
1.4	**Protección de los datos y de la privacidad de la información personal**			**Evidencia**	**Observacion**
	Existe la implementación y desarrollo de una política organizacional y de protección de datos, que haya sido comunicada a todo el personal implicado.	X		Documento de Política Organizacional Documento de requisitos legislativos.	
	Existen medidas técnicas y organizacionales apropiadas para proteger la información personal.		X	Documento de Política Organizacional Documento de requisitos legislativos.	
1.5	**Prevención en el mal uso de los recursos de tratamiento de la información**			**Evidencia**	**Observacion**
	Se adoptan acciones disciplinarias y/o legales apropiadas, cuando se identifica el uso de recursos para fines no autorizados.	X		Documentos de uso de recursos de tratamiento de la información Políticas de detección de intrusos Documento de requisitos legislativos, regulatorios y contractuales.	

Figura 54

Hoja de evaluación: Cumplimiento 3

	Los usuarios son conscientes del alcance preciso del acceso que se les permite y del monitoreo que se lleva a cabo para detectar un uso no autorizado.	X		Políticas de detección de intrusos Documento de requisitos legislativos, regulatorios y contractuales.	
	Existen mensajes de advertencia, que indique que el sistema al que se entra es privado y que no se permite acceso no autorizado.	X		Políticas de detección de intrusos Documento de requisitos legislativos, regulatorios y contractuales.	
1.6	**Regulación de los controles criptográficos**			**Evidencia**	**Observacion**
	Existe conformidad de restricciones en la importación y/o exportación de hardware y software para realizar funciones criptograficas con todos los acuerdos, leyes y regulaciones.	X		Documento de requisitos legislativos, regulatorios y contractuales. Documentos de las restricciones sobre el encriptado.	
	Las restricciones en el uso del encriptado estan en conformidad con todos los acuerdos, leyes y regulaciones.	X		Documento de requisitos legislativos, regulatorios y contractuales. Documentos de las restricciones sobre el encriptado.	
	Existen métodos obligatorios para acceder a la información que esté cifrada por hardware o software para proteger la confidencialidad de su contenido.		X	Documentos de los métodos para acceder a información cifrada	
2	Revisiones de la política de seguridad y de la conformidad técnica				
2.1	**Conformidad con la política de seguridad y los estándares.**			**Evidencia**	**Observacion**
	Existen revisiones regulares que aseguren el cumplimiento de las politicas de seguridad		X	Documentos de las revisiones de las políticas y normas de seguridad realizadas. Reportes de resultados de revisiones	
	Existe una evaluación de las causas de la no conformidad.		X	Documentos de las revisiones de las políticas y normas de seguridad realizadas.	
	Los resultados de las revisiones y de las acciones correctivas son grabados y mantenidos.	X		Reportes de resultados de revisiones	
	Se realiza un reporte de los resultados de las revisiones a las personas que llevan a cabo las revisiones independiente.	X		Documentos de las revisiones de las políticas y normas de seguridad realizadas. Reportes de resultados de revisiones	
2.2	**Comprobación de la conformidad técnica**			**Evidencia**	**Observacion**
	La comprobación de la conformidad técnica es realizada manualmente por un ingeniero de sistemas experimentado.	X		Documentación de las comprobaciones de conformidad técnica.	
	Las pruebas de vulnerabilidad son planeadas, documentadas y repetibles.	X		Documentos que sustenten las competencias y autorizaciones de los supervisores.	
	Las personas que realizan la comprobación de conformidad técnica son competentes y autorizadas.	X		Documentación de las comprobaciones de conformidad técnica. Documentos que sustenten las competencias y autorizaciones de los supervisores.	
3	Consideraciones sobre la auditoria de sistemas				

Figura 55

Hoja de evaluación: Cumplimiento 4

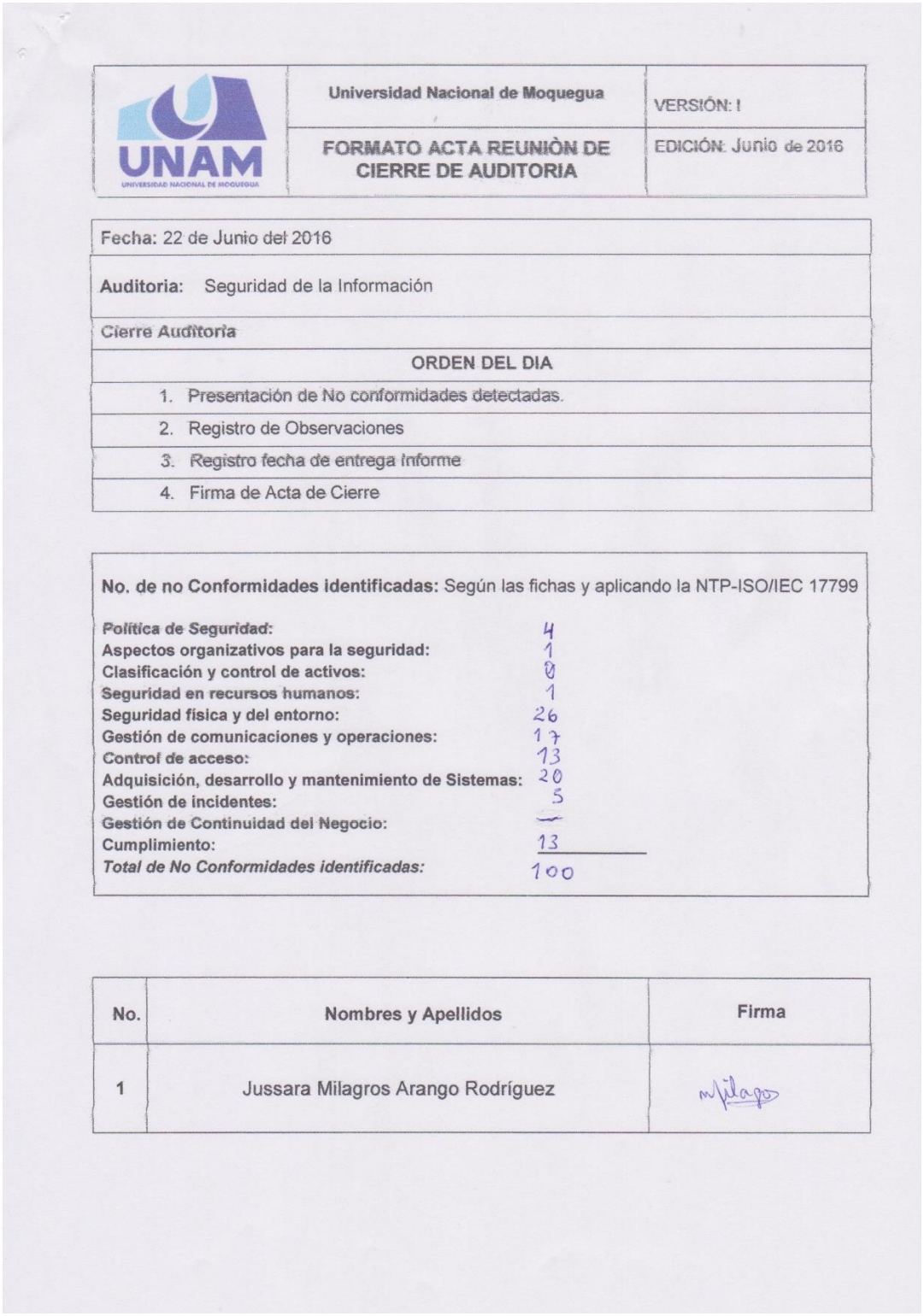
5.4	Controles de auditoria de sistemas			Evidencia	Observacion
	Los requisitos de auditoria se acuerdan con la gerencia apropiada.	X		Documento de procedimientos, requisitos y responsabilidades	
	El alcance de la auditoría es debidamente acordado y controlado.	X		Documento de procedimientos, requisitos y responsabilidades	
	Las verificaciones se limitan a accesos sólo de lectura al software y a los datos.	X		Documento de registro de accesos. Informes de auditoria.	
	Los accesos de sólo lectura, es permitido para copias aisladas de archivos del sistema y se borran al término de la auditoría.		X	Documento de registro de accesos. Informes de auditoria.	
	Los recursos de Tecnología de la Información son explícitamente identificados y puestos a disposición.	X		Documento de procedimientos, requisitos y responsabilidades Informes de auditoria.	
	Los requisitos para procesos especiales o adicionales son identificados y acordados.	X		Documento de procedimientos, requisitos y responsabilidades Informes de auditoria.	
	Los accesos estan regristrados y supervisados para producir un seguimiento de referencia.	X		Documento de procedimientos, requisitos y responsabilidades Documento de registro de accesos. Informes de auditoria.	
	Existe documentación de todos los procedimientos, reuisitos y responsabilidades.		X	Documento de procedimientos, requisitos y responsabilidades	
	Las personas que llevan a cabo la auditoría son independientes de las actividades auditadas.	X		Documento de procedimientos, requisitos y responsabilidades Informes de auditoria.	
3.2	Protección de las herramientas de auditoria de sistemas			Evidencia	Observacion
	Las herramientas de auditoria de sistemas estan separadas de los sistemas de desarrollo y de producción y no en librerías de cintas o áreas de los usuarios, salvo con nivel apropiado de protección adicional.	X		-	

GOBIERNO REGIONAL DE MOQUEGUA
SUB REGION ILO - UNIDAD EJECUTORA - 003

Ing. Christian Vizcarra Rodríguez
Encargado de Informática

Figura 56

Cierre de Auditoría



	Universidad Nacional de Moquegua	VERSIÓN: I
UNAM UNIVERSIDAD NACIONAL DE MOQUEGUA	FORMATO ACTA REUNIÒN DE CIERRE DE AUDITORIA	EDICIÓN: Junio de 2016

Fecha: 22 de Junio del 2016
Auditoria: Seguridad de la Información
Cierre Auditoria
ORDEN DEL DIA
1. Presentación de No conformidades detectadas.
2. Registro de Observaciones
3. Registro fecha de entrega Informe
4. Firma de Acta de Cierre

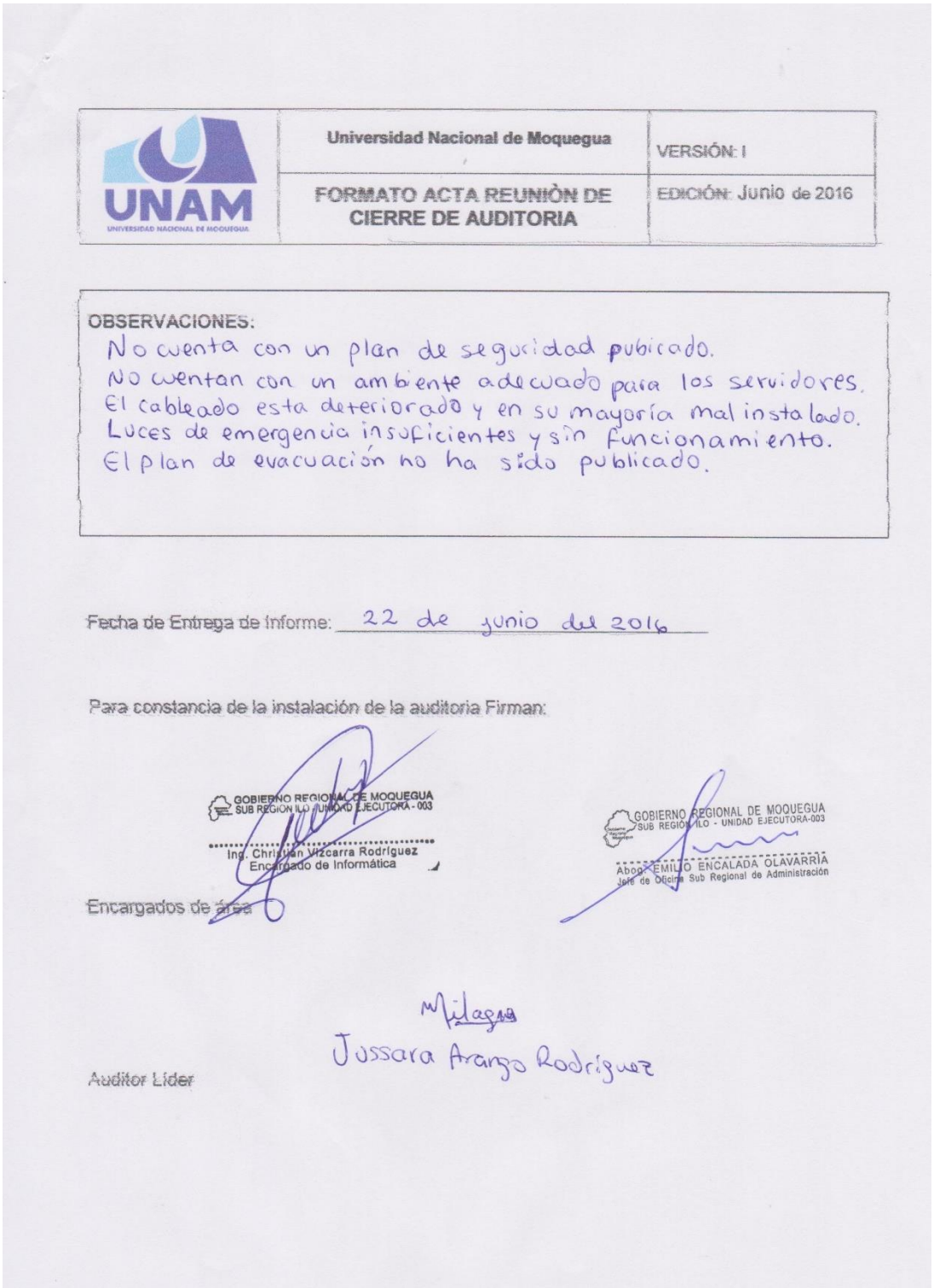
No. de no Conformidades identificadas: Según las fichas y aplicando la NTP-ISO/IEC 17799

Política de Seguridad:	4
Aspectos organizativos para la seguridad:	1
Clasificación y control de activos:	0
Seguridad en recursos humanos:	1
Seguridad física y del entorno:	26
Gestión de comunicaciones y operaciones:	17
Control de acceso:	13
Adquisición, desarrollo y mantenimiento de Sistemas:	20
Gestión de incidentes:	5
Gestión de Continuidad del Negocio:	—
Cumplimiento:	13
Total de No Conformidades identificadas:	100

No.	Nombres y Apellidos	Firma
1	Jussara Milagros Arango Rodríguez	mjilago

Figura 57

Cierre de Auditoría 2



UNAM UNIVERSIDAD NACIONAL DE MOQUEGUA	Universidad Nacional de Moquegua	VERSIÓN: I
	FORMATO ACTA REUNIÒN DE CIERRE DE AUDITORIA	EDICIÓN: Junio de 2016

OBSERVACIONES:

No cuenta con un plan de seguridad pubicado.
No cuentan con un ambiente adecuado para los servidores.
El cableado esta deteriorado y en su mayoría mal instalado.
Luces de emergencia insuficientes y sin funcionamiento.
El plan de evacuación no ha sido publicado.

Fecha de Entrega de Informe: 22 de junio del 2016

Para constancia de la instalación de la auditoria Firman:

GOBIERNO REGIONAL DE MOQUEGUA
SUB REGIÓN ILO - UNIDAD EJECUTORA - 003
Ing. Christian Vizcarra Rodriguez
Encargado de Informática

GOBIERNO REGIONAL DE MOQUEGUA
SUB REGIÓN ILO - UNIDAD EJECUTORA-003
Abog. EMILIO ENCALADA OLAVARRIA
Jefe de Oficina Sub Regional de Administración

Encargados de área

Milagros
Jussara Arango Rodriguez

Auditor Líder

FORMATO DE AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL UNAM

Formulario de autorización para la publicación electrónica en la página web del Repositorio Institucional de la Universidad Nacional de Moquegua, de conformidad con la Ley N° 30035 Ley que regula el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto y Resolución de Comisión Organizadora N° 041-2022-UNAM que aprueba el Reglamento que regula el Repositorio Institucional Digital de la UNAM.

1. DATOS DEL AUTOR

Nombres y Apellidos	: Jussara Milagros Arango Rodriguez
DNI/Carnet de Extranjería/Pasaporte N°	: 71579792
Correo electrónico	: jussara-ar@hotmail.com
Teléfono/Celular	: 988889667

2. GRADO, TITULO O ESPECIALIZACIÓN (Marque con una X)

Bachiller	Título Profesional	Magister	Doctor	Segunda Especialidad
	X			

3. TIPO DE PUBLICACIÓN (Marque con una X)

a) Articulo ( )
b) Tesis de pregrado ( )
c) Tesis de Maestría ( )
d) Tesis de Doctorado ( )
e) Monografía (X)
f) Reporte de caso científico o hallazgos ( )
g) Libro ( )
h) Parte de un libro ( )
i) Revisión ( )
j) Conferencia ( )
k) Presentación ( )
l) Artículo preliminar ( )
m) Articulo antes de ser publicado ( )
n) Artículo de prensa ( )
o) Documentos internos ( )
p) Imagen ( )
q) Documentos técnicos ( )
r) Ponencias presentadas en eventos científicos (Jornada, Congreso, Simposio Conferencias, etc.) ( )
s) Informes de suficiencia profesional ( )
t) Patentes producidas por académicos/as ( )

4. TIPO DE TRABAJO DE INVESTIGACIÓN (Marque con una X)

a) Tesis ( )
b) Trabajo de Investigación ( )
c) Trabajo de suficiencia profesional ( )
d) Trabajo académico (X)

5. DATOS DE LA PUBLICACION

a) Título : INFORME DE AUDITORÍA, APLICANDO LA NTP/ISO 17799, CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA SUBREGIÓN ILO
b) Campo del conocimiento OCDE (Indicar el código de clasificación OCDE de la obra : https://catalogos.concytec.gob.pe/vocabulario/ocde_ford.html) : 2.02.04
c) Fecha de publicación : 2022

6. DATOS DEL ASESOR:

a) Nombres y Apellidos : José Antonio Guzmán Valdivia
b) DNI/Pasaporte/Cédula : 40717092
c) ORCID : 0000-0002-4184-3421

FIRMA : .....

DOCUMENTO DE IDENTIDAD : 71579792
NOMBRES Y APELLIDOS : Jussara Milagros Arango Rodriguez

LICENCIAS

Licencia Estándar

Bajo los siguientes términos, autorizo el depósito de mi trabajo de investigación en el Repositorio Institucional Digital de la UNAM.

Con la autorización de depósito da mi trabajo de investigación, otorgo a la Universidad Nacional de Moquegua, una Licencia No Exclusiva para reproducir. distribuir, comunicar al público, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público mi trabajo de investigación (incluido el resumen), en formato fisico o digital, en cualquier medio, conocido o por conocerse, a través de los diversos servicios provistos por la Universidad, creados o por crearse, tales como el Repositorio Institucional Digital de la UNAM, Colección de Tesis, entre otros, en el Perú y en el extranjero, por el tiempo y veces que considere necesarias, y libre de remuneraciones.

En virtud de dicha Licencia, la UNIVERSIDAD NACIONAL DE MOQUEGUA, podrá reproducir mi trabajo de investigación en cualquier tipo de soporte y en más de un ejemplar, sin modificar su contenido, solo con los propósitos de seguridad, respaldo y preservación.

Declaro que el trabajo de investigación es una creación de mi autoría y exclusiva titularidad, o coautoría con titularidad compartida, y me encuentro facultado a conceder la presente licencia y, asimismo, garantizo que dicho trabajo de investigación no infringe derechos de autor de terceras personas.

La UNIVERSIDAD NACIONAL DE MOQUEGUA consignara el nombre del/los autor/es del trabajo de investigación, y no le hará ninguna modificación más de la permitida en la presente licencia.

Autorizo el depósito (marque con una X).

(__X__) **SI autorizo que se deposite inmediatamente.**

FIRMA : .....



DOCUMENTO DE IDENTIDAD : 71579792
NOMBRES Y APELLIDOS : Jussara Milagros Arango Rodriguez
FECHA : 24 de octubre del 2022