UNIVERSIDAD TÉCNICA DE MACHALA

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE ANÁLISIS DE SISTEMAS

“ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA”

TRABAJO PROBATORIO DEL COMPONENTE PRÁCTICO DEL EXAMEN DE GRADO DE CARÁCTER COMPLEXIVO PARA OPTAR POR EL TÍTULO DE ANALISTA DE SISTEMAS

AUTORA:

RUTH CECILIA MACIAS RIVERA

0704152024

MACHALA, OCTUBRE DE 2015

“ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA”

FRONTISPICIO

AUTORIA:

Yo, Macías Rivera Ruth Cecilia, como autora del presente trabajo probatorio del componente práctico del Examen de Grado de Carácter Complexivo, soy responsable de las ideas, conceptos, procedimientos y resultados vertidos en el mismo.

f…….

Macías Rivera Ruth Cecilia

C.I.: 0704152024

Correo electrónico: rukis_1304@hotmail.com

MACHALA, OCTUBRE DE 2015

“ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA”

Autor: Ruth Macías Rivera

Tutor: Ing. Wilmer Rivas Asanza

RESUMEN

La trabajo que se muestra a continuación, titulado: El establecimiento de entregables para la implementación de la norma ISO 27002: 2013 con respecto al dominio 9 11.14 para el data center de la UNEPBA (Unidad de Educación Privada Alexander Bilingüe), busca informar y orientar al lector todo lo que aplica las mejores prácticas en seguridad de la información; la misma que se crearon con el paso del tiempo y todas las estafas se están filtrando la información se imprime o no.

En primer lugar vamos a ver la introducción, donde las necesidades y evoluciones de las buenas prácticas de seguridad se destaca, por lo que se darán a conocer los objetivos generales que se han tenido en el desarrollo de este trabajo, entonces la institución problema que surge de la falta de normas y políticas de seguridad .

Luego se procede a dar a conocer más ampliamente sobre el tema que se está tratando, la presentación de la terminología básica y el apoyo a cada una de las partes de este trabajo.

Finalmente podemos ver los resultados en las políticas, procedimientos y plantillas para seguirse paso a paso en el departamento de sistemas de la unidad educativa, por lo que obtener una menor pérdida de información es detallada.

Palabras clave:

- ISO/IEC 27002
- SEGURIDAD DE LA INFORMACIÓN
- CONTROL DE ACCESO
- SEGURIDAD FISICA
- POLITICAS DE SEGURIDAD

“ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA”

Autor: Ruth Macías Rivera

Tutor: Ing. Wilmer Rivas Asanza

SUMMARY

The work that we will see below, entitled: Establish evidence to implement the ISO 27002 2013 regarding Environmental Control domain, and access computer systems maintenance, physical security and Acquisition Development for the Data Center of the UNEPBA (Educational Unit Bilingual particularly Alexander), seeks to inform and guide the reader in all that apply best practices in information security; the same as they were creating with the passage of time and all the scams are leaking information is printed or not.

First we have the introduction where we will highlight the needs and evolutions of good security practices, and also will release the general objectives which were taken in the development of this work, then we will raise the problem that arises from the lack of standards and security policies.

Then we proceed to make known more widely on the issue at hand, revealing basic terminology and supporting each of the parties to this work.

Finally we have the results where policies, procedures and templates to be followed step by step in the department of educational systems unit, so get to get less detailed data loss.

Keywords:

- ISO / IEC 27002
- SECURITY OF THE INFORMATION
- ACCESS CONTROL
- PHYSICAL SECURITY
- SECURITY POLITICS
- ISO / IEC 27002

ÍNDICE GENERAL

1. INTRODUCCION

“La gestión de seguridad de la información es un factor cada vez mas determinante en la competitividad de las organizaciones. La gestión del riesgo y el aseguramiento de la información se apoyan en la aplicación de normas internacionales como el estándar ISO/IES 27002.El proceso de la implementación de la norma y su gestión permanente se facilita a través del uso de software que en la actualidad es mayoritariamente comercial.” (Franco D. C. & Guerrero, 2013)

La propuesta de establecer evidencias para implementar los dominios Control de Acceso, Seguridad Física y Ambiental, Adquisición, Desarrollo y Mantenimiento de Sistemas Informáticos, es el objetivo principal del presente trabajo ya que actualmente la UNEPBA permite el libre acceso del personal a todas las áreas físicas, todo esto se debe a que no cuentan con una restricción para controlar el acceso al departamento y a su servidor de datos o información, con esto se lograra especificar requerimientos necesarios para mejorar un Sistema de Gestión de Seguridad de la información.

Es necesario realizar el establecimiento de las evidencias para la implementación en el Data Center, porque aparte de verificar las falencias se podrían aplicar los controles y políticas en base a las recomendaciones obtenidas para minimizar en el futuro que ocurran estos problemas, y como una forma de prevención para el tratamiento adecuado de Datos y el cuidado de la información.

1.1. MARCO CONTEXTUAL

La Unidad Educativa Particular Bilingüe Alexander se crea el 5 de Noviembre de 1982 en la ciudad de Machala, por iniciativa de la Dra. Josefina Rosales Echeverría, el Ministerio de Educación y Cultura autoriza el funcionamiento con los siguientes niveles y especializaciones: Pre-Primaria, Primaria y nivel medio. Así mismo, primero, segundo y tercero de Bachillerato en Comercio y Administración.

La estructura física de la unidad educativa está compuesta por un edificio en el que se encuentra el centro de datos, adicional a este posee 17 aulas, 1 laboratorio de informática y 1 laboratorio de ciencias.

La unidad educativa no cuenta con ningún estándar internacional implementado con respecto a la seguridad de la información, que ayude a proteger y resguardar la información. Esto provoca que personas externas tengan acceso a información importante para la unidad educativa, con la utilización de las nuevas tecnologías de información que pueden llegar a vulnerar información no protegida.

Existen estándares que proporcionan mecanismos de seguridad estudiados y puestos a prueba con excelentes resultados. Al seguir una recomendación de un estándar internacional concerniente a seguridad de la información es tener un protocolo en común para la medida de gestión de los riesgos informáticos.

.

1.2. PROBLEMA

“La seguridad informática es un tema muy amplio que se enfoca en poder entender que un riesgo y una vulnerabilidad se podrían englobar en una definición más informal que denota la diferencia entre riesgo y vulnerabilidad, de modo que se debe la Vulnerabilidad a una Amenaza y el Riesgo a un Impacto. La información (datos) se verá afectada por muchos factores, incidiendo básicamente en los aspectos de confidencialidad, integridad y disponibilidad de la misma. Desde el punto de vista de la empresa, uno de los problemas más importantes puede ser el que está relacionado con el delito o crimen informático, por factores externos e internos. Una persona no autorizada podría: Clasifica y desclasificar los datos, Filtrar información, Alterar la información, Borrar la información, Usurpar datos, Hojear información clasificada.” (VERGEL TRIGOS & SEPULVEDA ARENAS, 2015)

Una de las principales preocupaciones del departamento de sistemas de la unidad educativa, es el control de los riesgos que atentan contra la seguridad de la información de sus activos como entre estos, equipos informáticos, servicios, datos, recursos humanos y equipamiento auxiliar. Una observación rigurosa, se llegó a la conclusión, que los colaboradores de la unidad educativa (personal docente, administrativo y de servicio), cuentan con altos factores de inseguridad, fuga de información que si nose tratan adecuadamente pueden ocasionar posibles daños económicos y de prestigio para la unidad educativa, por tal razón se establece la siguiente pregunta ¿Cómo establecer formas de acceso, políticas y procedimientos de la información para la UNEPBA?

1.3. OBJETIVO GENERAL

Establecer entregables de la norma ISO 27002:2013, mediante un estudio de requerimientos y análisis para el establecimiento de normas de acceso de políticas y procedimientos en la UNEPBA.

2. DESARROLLO

2.1. Marco Teórico

2.1.1. Seguridad Informática

Consiste en garantizar que los recursos informáticos (Equipos, Software) estén disponibles a cualquier momento y sean utilizados de manera correcta, así como también asegurar la integridad y privacidad de la información. Se puede definir entonces a la seguridad informática como la disciplina que se relaciona a diversas técnicas, establecidas para prevenir, proteger y resguardar todo aquello susceptible de robo, perdida o daño, ya sea de manera personal, grupal o empresarial. “El objetivo de la seguridad informática será mantener la Integridad, Disponibilidad, Privacidad (sus aspectos fundamentales), Control y Autenticidad de la Información manejada por la computadora.” Todo lo que la seguridad informática dispone resguardar por todos aquellos riesgos presentes y que son motivo de análisis, se separan en dos escenarios, Seguridad Lógica y Seguridad Física. (Urgiles & Veintimilla, 2011)

2.1.2. Control de Acceso

“Este dominio tiene por objetivo controlar el acceso a los sistemas de información, servicios de información, bases de datos e instalaciones de procesamiento de información por medio de restricciones de acceso y excepciones. Esto ayuda a mantener protegida la información, contra accesos no autorizados y manipulación inadecuada de información por personal ajeno a la Universidad. Las políticas de seguridad que se establecen en este dominio procuran cumplir con los controles establecidos en el portal ISO, “Control de acceso”” (Torres Nunez, 2015)

2.1.3. Seguridad Física y Ambiental

“El objetivo de este dominio es minimizar los riesgos de daños en la información y las operaciones de la organización, por desastres naturales o por falta de control en la seguridad física ante desastres ambientales. Además, de establecer los perímetros de seguridad de las áreas de procesamiento de información. Las políticas de seguridad planteadas en este dominio se basan en los controles establecidos y publicados en el Portal ISO “La seguridad física y ambiental”” (Torres Nunez, 2015)

2.1.4. Adquisición, Desarrollo Y Mantenimiento De Los Sistemas De Información.

“El presente dominio tiene por objetivo la adquisición, desarrollo y mantenimiento de los sistemas de información que la empresa maneja, incluir controles para la validación de datos y correcto funcionamiento durante la adquisición y desarrollo. Aplicar procedimientos de control durante todo el ciclo de vida de desarrollo de proyectos incluyendo la protección de información crítica y sensible. Las políticas planteadas en este dominio aplican a todos los sistemas de información ya sean desarrollos propios o de terceros, estas políticas se basan en los controles publicados en el Portal ISO “Adquisición, desarrollo y mantenimiento de los sistemas de información”” (Torres Nunez, 2015)

2.1.5. Políticas De Seguridad

“Una política de seguridad es una técnica para gestionar los activos de una empresa para protegerlos apropiadamente, informando lo que está permitido, y que no lo está;

así como la responsabilidad de protección de los recursos que debería tener el personal.

“Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Esta a su vez establece reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos.”

El objetivo principal de las políticas de seguridad es proteger, prevenir y gestionar a una empresa, de las vulnerabilidades y riesgos a los que está expuesta, mediante normas, reglas y procedimientos precisos.” (CAPA & STALIN, 2015)

2.1.6. Norma ISO 27002

ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

La versión de 2013 del estándar describe los siguientes catorce dominios principales:

Organización de la Seguridad de la Información.

Seguridad de los Recursos Humanos.

Gestión de los Activos.

Control de Accesos.

Criptografía.

Seguridad Física y Ambiental.

Seguridad de las Operaciones.

Seguridad de las Comunicaciones.

Adquisición de sistemas, desarrollo y mantenimiento.: requisitos de seguridad de los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas.

Relaciones con los Proveedores.

Gestión de Incidencias que afectan a la Seguridad de la Información: gestión de las incidencias que afectan a la seguridad de la información; mejoras.

Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio: continuidad de la seguridad de la información; redundancias.

Conformidad: conformidad con requisitos legales y contractuales; revisiones

3. MARCO METODOLÓGICO

Mediante técnicas de investigación como la revisión de la documentación se ha desarrollado el caso de estudio:

Para establecer los entregables para la implementación de la norma ISO 27002:2013 se realizara los siguientes pasos:

1. Definición de requerimientos

Corresponde al levantamiento de todas las actividades relacionadas con los impactos que la organización pueda tener en relación con su seguridad de la información.

Pasos a seguir para definir los requerimientos:

- Definir el alcance y los objetivos
- Inventario de activos
- Identificar las amenazas y vulnerabilidades
- Identificar impactos
- Análisis y evaluación de riesgos
- Selección de controles
- Revisión de documentación de Políticas generales
- Revisión de documentación del sistema de información: Guía de usuario del sistema, Manual administrativo del sistema.
- Revisión del manual del diseño del sistema
- Revisión del manual de requerimientos
- Revisión del informe de evaluación de riesgos
- Revisión de los resultados de prueba del sistema

2. Elaboración de plantillas

Para la elaboración de las plantillas tomamos en cuenta el paso anterior porque mediante el análisis ya realizado elaboramos nuestra plantilla describiendo las principales funciones de la tecnología de información de la organización.

Esto corresponde al desarrollo de un documento que formalice como se deben realizar las actividades y que información es la que se debe retener como evidencia para dar conformidad a las políticas de seguridad informática.

Las plantillas se elaboran en base a

- Objetivos
- Funciones
- Políticas.

Objetivo

La construcción de la plantilla se basa en el objetivo de control, basado en todo sistema de seguridad informática.

Control: Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una compañía.

Funciones:

Describe los procesos que realiza la organización

- Políticas de control
- Servicios
- Registros
- Análisis de gestión
- Pruebas de funcionabilidad
- Identificación y clasificación

Política

La política de una organización es una declaración de principios generales que la empresa u organización se compromete a cumplir. En ella se dan una serie de reglas y directrices básicas acerca del comportamiento que se espera de sus empleados y fija las bases sobre cómo se desarrollarán los demás documentos manuales, procedimientos de la empresa.

Estructura de la plantilla

PROYECTO "ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):	UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"		
DENOMINACIÓN DEL HITO:	,		
NÚMERO DE HITO:		**ES UN HITO PRIORITARIO?**	
No.	**RESUMEN ACTIVIDADES REALIZADAS**	**VERIFICABLE INTERNO**	
		.	
PIE DE RESPONSABILIDAD			
FECHA ELABORACIÓN:			
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD:	**FIRMA:**		
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI:	**FIRMA:**		

3. Revisión de la plantilla

En esta etapa se debe realizar, preparar y desarrollar la revisión que avale que todos los procesos de tecnología informática se están cumpliendo y llevando a cabo adecuadamente.
En este proceso vamos a revisar si la información que contiene nuestra plantilla es necesaria para que sea aplicada.

La revisión también nos da la opción para la corrección de los datos.

4. Validar Plantillas

En esta etapa se busca verificar de manera adecuada a todos los registros de tecnología de información, para que todos sus procesos y controles estén disponibles para cualquier tipo de revisión
También se podrá verificar si los datos que están ahí son aplicables a la norma ISO 27002 de este proceso.

4. RESULTADOS

En base a los métodos y técnicas de estudio descritas anteriormente se procederá a establecer evidencias mediante la implementación de los dominios, control de acceso, seguridad física y ambiental, adquisición, desarrollo y mantenimiento de los sistemas informáticos.

4.1. Seguridad Física Y Ambiental

4.1.1. Establecer controles físicos de entrada.

Política

Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso.

Plantilla

PROYECTO "ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):	UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"		
DENOMINACIÓN DEL HITO:	Procedimiento para establecer controles físicos de entrada		
NÚMERO DE HITO:	*4,1,1*	**ES UN HITO PRIORITARIO?**	*SI*
No.	**RESUMEN ACTIVIDADES REALIZADAS**		**VERIFICABLE INTERNO**
1	• Los ingresos y egresos de personal a las instalaciones de la UNEPBA deben ser registrados. • El personal deberá portar el carnet que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la unidad. • El personal que sea contratado por temporadas y que tenga autorización de acceso deberán portar prendas distintivas que faciliten su identificación.		ESTABLECER CONTROLES FÍSICOS DE ENTRADA
PIE DE RESPONSABILIDAD			
FECHA ELABORACIÓN:	22 de Octubre del 2015		
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD: Ing. Doris Tenezaca 0704152056	**FIRMA:**		
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI: Cristina Lara 0704152036	**FIRMA:**		

4.1.2. Gestionar la seguridad de oficinas, despachos y recursos. Ver Anexo (1)

4.1.3. Realizar protección contra las amenazas externas y ambientales. Ver Anexo (2)

4.1.4. Realizar el trabajo en áreas seguras. Ver Anexo (3)

4.1.5. Gestionar la seguridad del cableado. Ver Anexo (4)

4.2. Control de Acceso

4.2.1. Realizar política de control de accesos. Ver Anexo (5)

4.2.2. Registro de Usuario. Ver Anexo (6)

4.2.3. Gestionar las altas/bajas en el registro de usuarios. Ver Anexo (7)

4.2.4. Analizar la gestión de los derechos de acceso con privilegios especiales. Ver Anexo (8)

4.2.5. Sistema de gestión de contraseñas. Ver Anexo (9)

4.3. Adquisición Desarrollo Y Mantenimiento De Sistemas De Información.

4.3.1. Analizar y especificar los requisitos de seguridad. Ver Anexo (10)

4.3.2. Validación de datos de salida. Ver Anexo (11)

4.3.3. Política sobre el uso de controles criptográficos. Ver Anexo (12)

4.3.4. Control del Software Operativo. Ver Anexo (13)

4.3.5. Verificar la externalización del desarrollo de software. Ver Anexo (13)

4.3.6. Procedimiento de control de cambios. Ver Anexo (14)

5. CONCLUSIONES

- Para poder realizar una política de seguridad primero se identificó la necesidad de crear las mismas.
- Las Políticas de Seguridad de la información se constituirán en los documentos oficiales de la institución, los cuales todo el personal o persona autorizada para el uso del mismo tiene que tenerlo en cuenta ante cualquier inquietud relacionada con la información.
- Las Políticas requieren la participación de todos los estudiantes, profesores, empleados administrativos, autoridades y demás miembros de la unidad educativa, quienes deberán ser concienciados de la importancia y necesidad de cumplir con las mismas. Ninguna política procedimiento, garantizará los principios de seguridad de la información si los usuarios directamente relacionados no están conscientes de la razón de ser de estas.
- Las Políticas de la Seguridad de la información de la unidad educativa, han sido elaboradas para salvaguardar la integridad de todos los componentes informáticos.
- Luego se analizó la política para poder hacer los pasos o los procedimientos para llegar a la misma.
- Se elaboró plantillas que han sido construidas en base a las necesidades de la unidad educativa, en la cual se incluyeron las políticas y procedimientos que se implementara en la unidad educativa.
- Se ha constituido como una herramienta sumamente útil a la hora de generar una propuesta, siendo importante adaptarse a la realidad de la unidad educativa.
- Este proyecto al momento de ser implementado tiene que hacerse retroalimentaciones constantes para conseguir que durante las iteraciones se vaya corrigiendo, puliendo y fortaleciendo.

6. REFERENCIAS BIBLIOGRÁFICAS

- Capa, L; Stalin, D., Diseño de un Sistema de Seguridad de la Información para la Compañía ACOTECNIC CIA LTDA. Basado en la norma NTE INEN ISO/IEC 27002, 2015, (http://dspace.ucuenca.edu.ec/jspui/bitstream/123456789/22371/1/tesis.pdf).
- Cruz, I.A.; David J., Planeación de la Seguridad de la Información corporativa sensible contra amenazas internas, 2011, (http://www.repositoriodigital.ipn.mx/bitstream/handle/123456789/12642/Trabajo%20de%20Investigaci%C3%B3n%20%20Jorge%20Alba%20Cruz.pdf?sequence=1)
- Franco D. C.; Guerrero, C. D., Sistema de Administración de Controles de Seguridad Informática basada en ISO/IEC 27002, 2013, (http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP239.pdf).
- Larrocha, E. R., MISILEON: Metodología que integra seguridad en ITIL evolucionada y orientada a la normalización, 2010. (http://e-spacio.uned.es/fez/eserv.php?pid=tesisuned:IngInf-Eruiz&dsID=Documento.pdf).

7. ANEXOS

7.1. Anexo (1) Gestionar la seguridad de oficinas, despachos y recursos.

Política

Se debería diseñar y aplicar un sistema de seguridad física a las oficinas e instalación de la organización.

Plantilla

<table>
<tr><td colspan="4">PROYECTO “ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA”</td></tr>
<tr><td colspan="4">INFORME DE CUMPLIMIENTO DE HITOS</td></tr>
<tr><td>ENTIDAD / (SIGLAS):</td><td colspan="3">UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"</td></tr>
<tr><td>DENOMINACIÓN DEL HITO:</td><td colspan="3">Procedimiento para gestionar la seguridad de oficinas, despachos y recursos,</td></tr>
<tr><td>NÚMERO DE HITO:</td><td>4,1,2</td><td>ES UN HITO PRIORITARIO?</td><td>SI</td></tr>
<tr><td>No.</td><td colspan="2">RESUMEN ACTIVIDADES REALIZADAS</td><td>VERIFICABLE INTERNO</td></tr>
<tr><td>1</td><td colspan="2">• Las aprobaciones de ingreso al centro de datos las debe ser dadas por los directivos de la unidad educativa.
• El jefe del departamento debe verificar que se tenga en stock el material o herramientas suficientes para en el caso de que exista algún daño y se pueda realizar el cambio inmediato
• El jefe de área debe certificar que el centro de datos y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgos de incendios.
• El jefe del departamento llevar control de la programación de los mantenimientos preventivos.</td><td>GESTIONAR LA SEGURIDAD DE OFICINAS, DESPACHOS Y RECURSOS.</td></tr>
<tr><td colspan="4">PIE DE RESPONSABILIDAD</td></tr>
<tr><td colspan="2">FECHA ELABORACIÓN:</td><td colspan="2">22 de Octubre del 2015</td></tr>
<tr><td colspan="2">NOMBRE y CÉDULA OFICIAL DE SEGURIDAD:
Ing. Doris Tenezaca
0704152056</td><td colspan="2">FIRMA:</td></tr>
<tr><td colspan="2">NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI:
Cristina Lara
0704152036</td><td colspan="2">FIRMA:</td></tr>
</table>

7.2. Anexo (2) Realizar protección contra las amenazas externas y ambientales. Política

Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentales.

Plantilla

PROYECTO "ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):	UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"		
DENOMINACIÓN DEL HITO:	Procedimiento para protección contra las amenazas externas y ambientales		
NÚMERO DE HITO:	*4,1,3*	**ES UN HITO PRIORITARIO?**	*SI*
No.	**RESUMEN ACTIVIDADES REALIZADAS**		**VERIFICABLE INTERNO**
1	• El jefe de área debe almacenar los materiales combustibles o peligrosos a una distancia prudente de las áreas protegidas. • El jefe de área debe ubicar los equipos de repuesto y soporte a una distancia prudente para evitar daños en caso de desastre que afecte las instalaciones principales. • El departamento de suministros deberá otorgar el equipo apropiado contra incendios y ubicarlo adecuadamente. • El departamento de mantenimiento deberá realizar mantenimiento de las instalaciones eléctricas y UPS. • Se deberá adoptar controles para minimizar el riesgo de amenazas físicas potenciales como robo, incendio, explosión, agua, polvo, humo.		PROTECCIÓN CONTRA LAS AMENAZAS EXTERNAS Y AMBIENTALES
PIE DE RESPONSABILIDAD			
FECHA ELABORACIÓN:	22 de Octubre del 2015		
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD: Ing. Doris Tenezaca 0704152056	**FIRMA:**		
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI: Cristina Lara 0704152036	**FIRMA:**		

7.3. Anexo (3) Realizar el trabajo en áreas seguras.

Política

Diseñar y aplicar procedimientos para el desarrollo e trabajos y actividades en áreas seguras.

Plantilla

PROYECTO "ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):	UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"		
DENOMINACIÓN DEL HITO:	Procedimiento para realizar el trabajo en áreas seguras		
NÚMERO DE HITO:	*4,1,4*	**ES UN HITO PRIORITARIO?**	*SI*
No.	**RESUMEN ACTIVIDADES REALIZADAS**		**VERIFICABLE INTERNO**
1	• El jefe de área debe dar a conocer al personal la existencia de un área segura. • El jefe de área deberá verificar todos los trabajos para evitar actividades maliciosas. • El jefe de área debe revisar periódicamente y dispondrá de bloqueos físicos de las áreas seguras vacías. • El jefe de área no permitirá el ingreso de cámaras, equipos de grabación, dispositivos móviles, etc., a menos de que estén autorizadas.		REALIZAR EL TRABAJO EN ÁREAS SEGURAS.
PIE DE RESPONSABILIDAD			
FECHA ELABORACIÓN:	22 de Octubre del 2015		
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD: Ing. Doris Tenezaca 0704152056	**FIRMA:**		
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI: Cristina Lara 0704152036	**FIRMA:**		

7.4. Anexo (4) Gestionar la seguridad del cableado.

Política

Los cables eléctricos de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños.

Plantilla

PROYECTO "ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):	UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"		
DENOMINACIÓN DEL HITO:	Procedimiento para establecer la seguridad en el cableado		
NÚMERO DE HITO:	*4,1,5*	**ES UN HITO PRIORITARIO?**	*SI*
No.	**RESUMEN ACTIVIDADES REALIZADAS**		**VERIFICABLE INTERNO**
1	• El departamento de centro de cómputo deberá proteger el cableado de la red contra la interceptación o daño. • El departamento de centro de cómputo deberá mantener separado los cables de energía de los cables de comunicaciones. • El departamento de centro de cómputo deberá identificar y rotular los cables de acuerdo a normas locales para evitar errores en el manejo. • El departamento de centro de cómputo deberá disponer de documentación, diseños y la distribución de conexiones de datos alámbricos/inalámbricos (locales y remotas), voz, eléctricas, polarizadas, etc. • El departamento de centro de cómputo deberá controlar el acceso a los módulos de cableado de conexión y cuartos de cableado.		ESTABLECER LA SEGURIDAD EN EL CABLEADO.
PIE DE RESPONSABILIDAD			
FECHA ELABORACIÓN:	22 de Octubre del 2015		
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD: Ing. Doris Tenezaca 0704152056	**FIRMA:**		
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI: Cristina Lara 0704152036	**FIRMA:**		

7.5. Anexo (5) Realizar política de control de accesos.

Política

Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la organización.

Plantilla

PROYECTO "ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):	UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"		
DENOMINACIÓN DEL HITO:	Procedimiento para establecer controles de acceso		
NÚMERO DE HITO:	*4,1,6*	**ES UN HITO PRIORITARIO?**	*SI*
No.	**RESUMEN ACTIVIDADES REALIZADAS**		**VERIFICABLE INTERNO**
1	• El departamento de centros de datos gestionara los accesos de los usuarios a los sistemas de información, asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados. • El departamento de centros de datos definirá responsabilidades para identificar, gestionar y mantener perfiles de los custodios de información. • El departamento de centros de datos definirá claramente los autorizadores de los permisos de acceso a la información.		ESTABLECER CONTROLES DE ACCESO
PIE DE RESPONSABILIDAD			
FECHA ELABORACIÓN:	22 de Octubre del 2015		
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD: Ing. Doris Tenezaca 0704152056	**FIRMA:**		
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI: Cristina Lara 0704152036	**FIRMA:**		

7.6. Anexo (6) Registro de Usuario.

Política

Establecer un procedimiento formal documentado y difundido, en el cual se evidencie detalladamente los pasos y responsables para:

- Definir el administrador de accesos que debe controlar los perfiles y roles.

Plantilla

PROYECTO "ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):	UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"		
DENOMINACIÓN DEL HITO:	Registro de usuario establecido		
NÚMERO DE HITO:	*4,1,7*	**ES UN HITO PRIORITARIO?**	*SI*
No.	**RESUMEN ACTIVIDADES REALIZADAS**		**VERIFICABLE INTERNO**
1	Elaboración de un REGISTRO DE USUARIOS PARA EL CONTROL DE ACCESO, donde se registra información para establecer responsabilidades de las actividades control de acceso		REGISTRO DE USUARIOS PARA EL CONTROL DE ACCESO
PIE DE RESPONSABILIDAD			
FECHA ELABORACIÓN:	22 de Octubre del 2015		
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD: Ing. Doris Tenezaca 0704152056	**FIRMA:**		
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI: Cristina Lara 0704152036	**FIRMA:**		

Verificable Interno

REGISTRO DE USUARIOS PARA EL CONTROL DE ACCESO

HITO 4.1.7

Administrador de Accesos	

Solicitud de requirimiento de accesos			
Solicitante:			
Jefe del Dpto:			
Implementa el Requerimiento			
Existe acuerdo de confidencialidad firmado por el solicitante:		si ☐	no ☐

Historial de asignacion de accesos		
Fecha	Estado del Acceso	Descripcion

	Personal de Tecnología Administrador de accesos	Jefe del Dpto
Copia a:	Jefe Tecnología de la Información Oficial de Seguridad de la Información	

El jefe del área de tecnología debe asignar de su personal un administrador de accesos quien se encarga de aplicar en los sistemas las solicitudes de permisos y accesos.

El jefe departamental es quien solicita al área de tecnología los permisos de los usuarios autorizados.

El jefe de personal debe enviar copias de los acuerdos de confidencialidad a los jefes departamentales correspondientes y al jefe del área de tecnología

El oficial de seguridad de la información debe verificar que los permisos solicitados sean los que están asignados.

Para definir los permisos es importante que el área de tecnología tenga un listado de todos los sistemas con los permisos se les puede asignar a cada sistema, para que el jefe departamental determine los permisos que le corresponde al usuario, para mayor efectividad de este proceso sería que esta actividad se lo haga en presencia de los 2 funcionarios

Para que se aplique los permisos de los usuarios es indispensable la presencia del documento de acuerdo de confidencialidad firmado por el usuario.

Para evidencia es necesario REGISTRAR EL CONTROL DE ACCESO en la ficha de este hito, de esta manera queda un historial para cada usuario de los permisos asignados.

7.7. Anexo (7) Gestionar las altas/bajas en el registro de usuarios.

Política

Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.

Plantilla

<table>
<tr><td colspan="4">PROYECTO “ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA”</td></tr>
<tr><td colspan="4">INFORME DE CUMPLIMIENTO DE HITOS</td></tr>
<tr><td>ENTIDAD / (SIGLAS):</td><td colspan="3">UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"</td></tr>
<tr><td>DENOMINACIÓN DEL HITO:</td><td colspan="3">Procedimiento para gestionar las altas/bajas en el registro de usuarios</td></tr>
<tr><td>NÚMERO DE HITO:</td><td>4,1,8</td><td>ES UN HITO PRIORITARIO?</td><td>SI</td></tr>
<tr><td>No.</td><td colspan="2">RESUMEN ACTIVIDADES REALIZADAS</td><td>VERIFICABLE INTERNO</td></tr>
<tr><td>1</td><td colspan="2">• La petición de modificaciones de propiedades de una cuenta de usuario de la aplicación, las solicitara el responsable del área.
• El responsable del área del departamento de centro de datos tras comprobar los cambios solicitados, autorizará las modificaciones solicitadas y realizara los cambios desde este nuevo módulo de mantenimiento de usuarios.
• El departamento de centro de datos deberá crear una notificación a través del sistema con asunto cambio de perfil de usuario, dirigida al área de sistemas.
• A través del módulo de mantenimiento de usuarios se podrá consultar, actualizar o dar de alta nuevos usuarios para la aplicación.</td><td>REGISTRO DE LAS ALTAS/BAJAS.</td></tr>
<tr><td colspan="4">PIE DE RESPONSABILIDAD</td></tr>
<tr><td colspan="2">FECHA ELABORACIÓN:</td><td colspan="2">22 de Octubre del 2015</td></tr>
<tr><td colspan="2">NOMBRE y CÉDULA OFICIAL DE SEGURIDAD:
Ing. Doris Tenezaca
0704152056</td><td colspan="2">FIRMA:</td></tr>
<tr><td colspan="2">NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI:
Cristina Lara
0704152036</td><td colspan="2">FIRMA:</td></tr>
</table>

7.8. Anexo (8) Analizar la gestión de los derechos de acceso con privilegios especiales.

Política

Controlar la asignación de privilegios a través de un proceso formal de autorización.

Plantilla

PROYECTO "ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):	UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"		
DENOMINACIÓN DEL HITO:	Asignación de privilegios a través de un proceso formal de autorización, controlado		
NÚMERO DE HITO:	*4,1,9*	**ES UN HITO PRIORITARIO?**	*SI*
No.	**RESUMEN ACTIVIDADES REALIZADAS**	**VERIFICABLE INTERNO**	
1	Elaboración de un CONTROL DE ASIGNACION DE PRIVILEGIOS A TRAVES DE UN PROCESO FORMAL DE AUTORIZACION El jefe del área de tecnología debe asignar de su personal un administrador de accesos quien se encarga de aplicar en los sistemas las solicitudes de permisos y accesos. El jefe departamental es quien solicita al área de tecnología los permisos de los usuarios autorizados. El jefe de personal debe enviar copias de los acuerdos de confidencialidad a los jefes departamentales correspondientes y al jefe del área de tecnología El oficial de seguridad de la información debe verificar que los permisos solicitados sean los que están asignados.	CONTROL DE ASIGNACION DE PRIVILEGIOS A TRAVES DE UN PROCESO FORMAL DE AUTORIZACION	
PIE DE RESPONSABILIDAD			
FECHA ELABORACIÓN:	22 de Octubre del 2015		
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD: Ing. Doris Tenezaca 0704152056	**FIRMA:**		
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI: Cristina Lara 0704152036	**FIRMA:**		

7.9. Anexo (9) Sistema de gestión de contraseñas

Política

Generar un procedimiento formal para la administración y custodia de las contraseñas de acceso de administración e información crítica de la institución.

Plantilla

PROYECTO "ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):	UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"		
DENOMINACIÓN DEL HITO:	Procedimiento formal para la administración y custodia de las contraseñas de acceso, generado.		
NÚMERO DE HITO:	*4,1,10*	**ES UN HITO PRIORITARIO?**	*SI*
No.	**RESUMEN ACTIVIDADES REALIZADAS**	**VERIFICABLE INTERNO**	
1	Elaboración de un procedimiento para la administración y custodia de las contraseñas de acceso, las contraseñas son usadas con múltiples propósitos en la UNEPBA, como pueden ser las contraseñas de cuentas de usuario del sistema portuario, servicios Web, cuentas de correo electrónico, protectores de pantalla en los recursos de los usuarios, administración de dispositivos remotos, etc… Se debe poner especial atención en la selección de contraseñas seguras para la autentificación en todos los recursos y servicios de la UNEPBA. Las contraseñas no deben ser almacenadas por escrito nunca. Los usuarios deben custodiar las claves en archivos encriptados, si lo hacen en pendrive tiene que estar ubicado bajo llaves.	PROCEDIMIENTO PARA LA ADMINISTRACIÓN Y CUSTODIA DE LAS CONTRASEÑAS DE ACCESO.	
PIE DE RESPONSABILIDAD			
FECHA ELABORACIÓN:	22 de Octubre del 2015		
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD: Ing. Doris Tenezaca 0704152056	**FIRMA:**		
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI: Cristina Lara 0704152036	**FIRMA:**		

Verificable Interno

PROCEDIMIENTO PARA LA ADMINISTRACION Y CUSTODIA DE LAS CONTRASEÑAS DE ACCESO

1.- PROPOSITO

Las contraseñas son un aspecto fundamental de la seguridad de los recursos informáticos, es la primera línea de protección para el usuario. Una contraseña mal elegida o protegida puede resultar en un agujero de seguridad para toda la organización. Por ello, todos los usuarios de la UNEPBA son responsables de velar por la seguridad de las contraseñas seleccionadas por ellos mismos para el uso de los distintos servicios ofrecidos por la UNEPBA.

Es importante la protección de dichas contraseñas, y el cambio frecuente de las mismas.

2.- DESARROLLO

Todas las contraseñas de cuentas que den acceso a recursos y servicios de la UNEPBA deben ser cambiados al menos una vez cada seis meses,, se recomienda cambiarla con mayor frecuencia y también siempre que el usuario sospeche que la seguridad de su contraseña pueda haber sido comprometida.

Las contraseñas no deben ser incluidas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica. Tampoco deben ser comunicadas las contraseñas en conversaciones telefónicas.

En la medida de lo posible, las contraseñas serán generadas automáticamente con las características recomendadas en esta política y se les comunicará a los usuarios su contraseña siempre en estado “expirado” para obligar al usuario a cambiarla en el primer uso que hagan de la cuenta o servicio.

3.- SELECCIÓN Y CUSTODIA DE CONTRASEÑAS

Las contraseñas son usadas con múltiples propósitos en la UNEPBA, como pueden ser las contraseñas de cuentas de usuario del sistema portuario, servicios Web, cuentas de correo electrónico, protectores de pantalla en los recursos de los usuarios, administración de dispositivos remotos, etc… **Se debe poner especial atención en la selección de contraseñas seguras para la autentificación en todos los recursos y servicios de la UNEPBA.**

La seguridad de este tipo de autentificación se basa en dos premisas:

1- La contraseña personal sólo la conoce el usuario.

2- La contraseña es lo suficientemente “fuerte” para no ser descifrada.

Las contraseñas no deben ser almacenadas por escrito nunca.

Los usuarios deben custodiar las claves en archivos encriptados, si lo hacen en pendrive tiene que estar ubicado bajo llaves.

3.2.- Recomendaciones para la protección de la contraseña

No revele su contraseña por teléfono a NADIE, incluso aunque le hablen en nombre del servicio de informática o de un superior suyo en la organización.

No revele la contraseña en mensajes de correo electrónico ni a través de cualquier otro medio de comunicación electrónica.

Nunca escriba la contraseña en papel y lo guarde. Tampoco almacene contraseñas en ficheros de ordenador sin encriptar o proveerlo de algún mecanismo de seguridad.

No revele su contraseña a sus superiores, ni a sus colaboradores.

No hable sobre una contraseña delante de otras personas.

No revele su contraseña en ningún cuestionario o formulario, independientemente de la confianza que le inspire el mismo.

No comparta la contraseña con familiares.

No revele la contraseña a sus compañeros cuando se marche de vacaciones.

No utilice la característica de “*Recordar Contraseña*” existente en algunas aplicaciones (Outlook, Netscape, Internet Explorer).

Si sospecha que una cuenta o su contraseña pueden haber sido comprometidas, comuníquelo al responsable de la seguridad de la información y cambie las contraseñas de todas sus cuentas.

Cambie las contraseñas con la frecuencia recomendada para cada tipo de cuenta y servicio.

3.3.- Estándares de desarrollo de aplicaciones

Los desarrolladores de aplicaciones informáticas para la UNEPBA y que gestionen sus propios mecanismos de autentificación mediante contraseñas, deben asegurarse de que sus programas contienen las siguientes precauciones en términos de seguridad respecto de la selección y uso de contraseñas:

Deben proveer de un mecanismo para expirar las contraseñas y obligar a los usuarios al cambio de la misma.

Se debe limitar el número de intentos de accesos sin éxito consecutivos.

7.10. Anexo (10) Analizar y especificar los requisitos de seguridad.

Política

Definir los requerimientos de seguridad. Por ejemplo: criptografía, control de sesiones, etc.

Plantilla

PROYECTO "ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):	UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"		
DENOMINACIÓN DEL HITO:	Definir los requerimientos de seguridad. Por ejemplo: criptografía, control de sesiones, etc.		
NÚMERO DE HITO:	*4,1,11*	**ES UN HITO PRIORITARIO?**	*SI*
No.	**RESUMEN ACTIVIDADES REALIZADAS**		**VERIFICABLE INTERNO**
1	La UNEPBA, a través del Área de Tecnología de la Información, ha contratado la implementación de sistemas de información, sin embargo, son sistemas de información que cumplen con REQUERIMIENTOS DE SEGURIDAD técnicos, inicialmente contratados. En proyectos futuros, de implementación o actualización de sistemas de información, que el Área de Tecnología implemente o gestione, deberán, a más de los REQUERIMIENTOS DE SEGURIDAD ya existentes, depurarse y definirse requerimientos más exigentes de acuerdo al avance tecnológico en seguridades.		Manuales técnicos de los sistemas de la UNEPBA
PIE DE RESPONSABILIDAD			
FECHA ELABORACIÓN:	22 de Octubre del 2015		
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD: Ing. Doris Tenezaca 0704152056	**FIRMA:**		
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI: Cristina Lara 0704152036	**FIRMA:**		

7.11. Anexo (11) Validación de datos de salida.

Política

Desarrollar procedimientos para responder a las pruebas de validación de la salida de datos.

- **Plantilla**

PROYECTO "ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):	UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"		
DENOMINACIÓN DEL HITO:	Procedimientos para responder a las pruebas de validación de salidas, desarrollados.		
NÚMERO DE HITO:	*4,1,12*	**ES UN HITO PRIORITARIO?**	*SI*
No.	**RESUMEN ACTIVIDADES REALIZADAS**		**VERIFICABLE INTERNO**
1	Elaboración de PROCEDIMIENTO PARA RESPONDER A LAS PRUEBAS DE VALIDACION DE DATOS La empresa que desarrolle el sistema debe planificar las pruebas de validación de datos en el cual se detalle los datos de entrada y los resultados esperados. Debe planificar las fechas de la realización de las pruebas con la aceptación de participación de los usuarios. El usuario es la persona indicada para que ingrese los datos de entrada verificando que los datos están validados para que la información que se almacene en la base de datos garantice la integridad de los datos. La empresa debe registrar la aceptación de las pruebas. El área de tecnología de la información debe aprobar las pruebas desarrolladas.		PROCEDIMIENTO PARA RESPONDER A LAS PRUEBAS DE VALIDACION DE DATOS.
PIE DE RESPONSABILIDAD			
FECHA ELABORACIÓN:	22 de Octubre del 2015		
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD: Ing. Doris Tenezaca 0704152056	**FIRMA:**		
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI: Cristina Lara 0704152036	**FIRMA:**		

7.12. Anexo (12) Política sobre el uso de controles criptográficos.

Política

Identificar el nivel requerido de protección de datos que se almacenara en el sistema considerando: el tipo, fortaleza y calidad del algoritmo cifrado (encriptación) requerido.

- **Plantilla**

PROYECTO "ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):	UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"		
DENOMINACIÓN DEL HITO:	*Uso de programas utilitarios restringidos y controlados*		
NÚMERO DE HITO:	*4,1,12*	**ES UN HITO PRIORITARIO?**	*SI*
No.	**RESUMEN ACTIVIDADES REALIZADAS**		**VERIFICABLE INTERNO**
1	Elaboración de POLITICAS DE IDENTIFICACION, AUTORIZACION Y AUTENTICACION PARA PROGRAMAS UTILITARIOS El área de tecnología de la información debe configurar para no permitir que los usuarios activen las utilidades del sistema, al intentar activar alguna utilidad el sistema solicite clave del administrador Si un usuario necesita activar alguna utilidad, el jefe departamental deberá solicitar al área de tecnología de la información la activación con la debida justificación, indicando el tiempo. El área de tecnología de la información monitoreara el tiempo de la activación de la utilidad para cuando se cumpla desactivar. • El área de tecnología de la información monitoreara que los recursos consumidos por la utilidad no genere riesgos para la institución.		POLITICAS DE IDENTIFICACION, AUTORIZACION Y AUTENTICACION PARA PROGRAMAS UTILITARIOS.
PIE DE RESPONSABILIDAD			
FECHA ELABORACIÓN:	22 de Octubre del 2015		
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD: Ing. Doris Tenezaca 0704152056	**FIRMA:**		
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI: Cristina Lara 0704152036	**FIRMA:**		

7.13. Anexo (13) Control del software operativo

Política

Definir el proceso de paso a producción para cada sistema.

Plantilla

PROYECTO "ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):	UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"		
DENOMINACIÓN DEL HITO:	Mínima alteración en los procesos, durante la implementación, garantizada.		
NÚMERO DE HITO:	*4,1,13*	**ES UN HITO PRIORITARIO?**	*SI*
No.	**RESUMEN ACTIVIDADES REALIZADAS**	**VERIFICABLE INTERNO**	
1	Elaboración de un formato de registro de informe de paso de pruebas a producción con detalle de cambios y acciones a ejecutar, la persona que registra es el implementador de cambios y lo autoriza el Jefe del área de tecnología.	REGISTRO DE INFORME DE PASO PRUEBAS A PRODUCCION CON DETALLE A CAMBIOS Y ACCIONES A EJECUTAR.	
PIE DE RESPONSABILIDAD			
FECHA ELABORACIÓN:	22 de Octubre del 2015		
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD: Ing. Doris Tenezaca 0704152056	**FIRMA:**		
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI: Cristina Lara 0704152036	**FIRMA:**		

7.14. Anexo (14) Procedimiento de control de cambio.

Política

Garantizar que la implementación se llevara a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.

Plantilla

PROYECTO "ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÒN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):	UNIDAD EDUCATIVA PARTICULAR BILINGÜE ALEXANDER "UNEPBA"		
DENOMINACIÓN DEL HITO:	Mínima alteración en los procesos, durante la implementación, garantizada.		
NÚMERO DE HITO:	*4,1,14*	**ES UN HITO PRIORITARIO?**	*SI*
No.	**RESUMEN ACTIVIDADES REALIZADAS**	**VERIFICABLE INTERNO**	
1	Elaborar un documento de registro de tratamiento de cambios, donde se registra el impacto esperado sobre el sistema existente, la no disponibilidad temporal de la aplicación.	Registro de tratamiento de cambios	
PIE DE RESPONSABILIDAD			
FECHA ELABORACIÓN:	22 de Octubre del 2015		
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD: Ing. Doris Tenezaca 0704152056	**FIRMA:**		
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI: Cristina Lara 0704152036	**FIRMA:**		

Verificable Interno

REGISTRO DE TRATAMIENTO DE CAMBIOS

ID Cambios	
Fecha y hora del tratamiento	
Nombre del Funcionario	
Departamento	

Estado:

Registrado	
En ejecución	
Suspendido	
Resuelto	
Cerrado	

CLASIFICACIÓN DEL CAMBIO		
Tipo de servicio afectado	Nivel de severidad	
EJM: Red, Internet, Datos, DB Oracle, Oracle Web Logic, Pagina Web, Biometricos, FO, utp, switch, Pérdida del servicio de red del equipo o de las prestaciones, Mal funcionamiento del software o del hardware, etc.	Impacto del cambio	Impacto en el Tiempo
	Alto	
	Medio	
	Bajo	
Nivel de autorización para la Implantación del cambio:(hito 8.11.4)		

Llenar sólo en el caso de que se produjeran varios eventos simultáneos

Urgencia o prioridad de atención del incidente	Alto	Medio	Bajo

Listar las tareas a realizar hito 8.11.3		
Fecha	Tarea	Responsable
Tareas a realizar en el ambiente de pruebas hito 8.11.10		
Estradas	Tarea	Resultados Esperados hito 8.11.8
Solicitud de autorizacion al propietario de la información hito 8.11.5 hito 8.11.11		
Fecha	Descripcion	Firma

Notificacion a usuarios hito 8.11.6		
Fecha	Usuario notificado	Firma

Solicitud de acceso remoto hito 8.11.7			
fecha	hora inicio	hora fin	Acciones de cambio, pruebas y configuracion

Impacto sobre la aplicación informática (Hito 8.11.14)

Mucho impacto al software base

Si ☐	No ☐
Si la respuesta es Si, detallar un plan de contingencia , posibles riesgos	

_____
Personal de Tecnología
Encargado

_____
Responsable de Seguridad
de la Información

Copia a: Jefe Tecnología de la Información
Oficial de Seguridad de la Información

CESIÓN DE DERECHOS DE AUTOR

Yo, MACIAS RIVERA RUTH CECILIA, con C.I. 0704152024, estudiante de la carrera de ANÁLISIS DE SISTEMAS de la UNIDAD ACADÉMICA DE INGENIERÍA CIVIL de la UNIVERSIDAD TÉCNICA DE MACHALA, en calidad de Autora del siguiente trabajo de titulación "ESTABLECIMIENTO DE ENTREGABLES PARA IMPLEMENTACIÓN DE ISO 27002:2013, RESPECTO AL DOMINIO 9, 11,14, PARA EL DATA CENTER DE LA UNEPBA"

- Declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional. En consecuencia, asumo la responsabilidad de la originalidad del mismo y el cuidado al remitirme a las fuentes bibliográficas respectivas para fundamentar el contenido expuesto, asumiendo la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera EXCLUSIVA.

- Cedo a la UNIVERSIDAD TÉCNICA DE MACHALA de forma NO EXCLUSIVA con referencia a la obra en formato digital los derechos de:

  a. Incorporar la mencionada obra al repositorio digital institucional para su democratización a nivel mundial, respetando lo establecido por la Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0), la Ley de Propiedad Intelectual del Estado Ecuatoriano y el Reglamento Institucional.

  b. Adecuarla a cualquier formato o tecnología de uso en internet, así como incorporar cualquier sistema de seguridad para documentos electrónicos, correspondiéndome como Autor(a) la responsabilidad de velar por dichas adaptaciones con la finalidad de que no se desnaturalice el contenido o sentido de la misma.

Machala, 27 de noviembre de 2015

MACIAS RIVERA RUTH CECILIA
C.I. 0704152024