Ingenium | Vol. 5 (1), enero-junio 2020 | ISSN en línea 2519-1403
Doi: http://dx.doi.org/10.18259/ing.2020002

LECCIONES APRENDIDAS EN SEGURIDAD DE LA INFORMACIÓN EN UNA ALCALDÍA DE CATEGORÍA 1

Lessons learned in information security in a Category 1 Mayor's Office

Dougglas Hurtado Carmona[1]*, Israel Escobar Hernandez[1]

[1] Programa de Ingeniería de Sistemas, Politécnico de la Costa Atlántica, Barranquilla, Colombia

* Autor de correspondencia: dhurtadoc@pca.edu.co

Resumen

El trabajo de realizar el aseguramiento de la seguridad de la información en una alcaldía Categoría 1 es un ente complejo que presenta sus propios retos, debido al gran flujo de información que se mantiene derivado a la alta sinergia entre los procesos que demanda el ejercicio público en una ciudad, en el escenario de la modernización que se hace necesario para estar acorde con la utilización de las nuevas tendencias tecnológicas que le generen valor agregado en utilidad y garantía para sus usuarios y clientes. En esta línea de acción, se presentan las lecciones a tener en cuenta al realizar un diagnóstico de la seguridad de la información en las distintas dependencias bajo el cumplimiento de la norma ISO/IEC 27001.

Palabras clave: Lecciones aprendidas, seguridad informática, sector público.

Abstract

The job of performing information security assurance in a Category 1 mayor's office is a complex entity that presents its own challenges, due to the large flow of information that remains derived from the high synergy between the processes that public practice demands in a city, in the scenario of modernization that is necessary to be in accordance with the use of new technological trends that generate added value in utility and guarantee for its users and customers. In this line of action, the lessons to be taken into account that originate when carrying out an information security diagnosis in the different dependencies are presented, in compliance with the ISO / IEC 27001 standard.

Keywords: Lessons learned, computer security, public sector.

I. INTRODUCCIÓN

Dentro del marco del convenio interadministrativo celebrado entre el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MiniTic) y una alcaldía de categoría 1, con el objeto de implementar el *Manual 3.0 de gobierno en línea,* se han ejecutado distintos proyectos con el fin de ejecutar los diferentes lineamientos descritos en dicho manual para las entidades del orden nacional de la República de Colombia [1].

Entre los proyectos a desarrollarse, en este convenio, está el que corresponde al área de la Seguridad de la Información, asignado a la Oficina de Modernización, que tiene como objetivo determinar el estado de la seguridad de la infor-

mación en una alcaldía de categoría 1, realizando un diagnóstico inicial, un establecimiento y alcance del sistema de gestión de seguridad de la información (SGSI), implementación del SGSI y una auditoría interna del SGSI bajo la norma ISO/IEC 27001.

El alcance del proyecto estaría enmarcado bajo el enfoque de la norma ISO/IEC 27001, porque se considera que es necesario especificar los requisitos adecuados para la implementación de los controles de seguridad adaptados a las necesidades de una alcaldía de categoría 1. Asimismo, se pretende establecer los requisitos generales necesarios para crear un sistema de gestión documentado con las actividades totales de negocio de la alcaldía y los riesgos a los que se enfrenta.

En definitiva, este proyecto determinará las obligaciones que debe adoptar la alcaldía para establecer, implementar, revisar y mejorar el sistema de gestión de seguridad de la información (SGSI). Este proyecto se desarrolló en el segundo semestre del año 2012, en cuatro etapas o fases: (i) Determinación del estado actual de la seguridad de la información, (ii) Establecimiento y alcance del SGSI, (iii) Implementación del SGSI y (iv) Auditoría interna del SGSI bajo la norma ISO 27001.

La etapa del proyecto denominada Diagnóstico inicial y oportunidades de mejora del sistema de gestión de seguridad de la información tuvo como objetivo determinar el estado actual de la seguridad de la información, así como definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información. Además, este diagnóstico se aplica a todo el Sistema de Gestión de Seguridad de la Información (SGSI) que depende de la Gerencia de Sistemas de la alcaldía [2, p. 1].

En la etapa Auditoría interna del SGSI bajo la norma ISO 27001, se verificará el cumplimiento de la norma procedente de la gestión de la seguridad de la información en la alcaldía. En esencia, es una actividad de análisis que evalúa las actividades para determinar posibles errores y establecer pautas para corregirlos [3, p. 3]. Luego de efectuar las correcciones detectadas en el diagnóstico inicial, se vuelve a realizar el proceso de auditoría con el fin de establecer los avances obtenidos al implementar, en su primera fase, el Sistema de Gestión de Seguridad de la Información en la Alcaldía. Al tener estos dos escenarios, se comparan y se trazan pautas a seguir con el fin de permitir el fortalecimiento del aseguramiento de la seguridad de la información de una alcaldía de categoría 1.

II. LECCIONES APRENDIDAS

Durante la realización del proyecto en seguridad de la información en una alcaldía de categoría 1, se identificaron, detectaron, analizaron y evaluaron buenas y malas prácticas en el manejo y tratamiento de la información en los distintos dominios de control especificados por la Norma ISO/IEC 2001.

El Proyecto Mercados Centroamericanos para la Biodiversidad (CAMBio, por sus siglas en inglés) ha definido una lección aprendida como

> una buena práctica de trabajo, experiencia o enfoque innovador que es obtenido y compartido para promover aplicaciones repetidas. Una lección aprendida puede también ser una mala práctica de trabajo o experiencia adversa que es obtenida y compartida para evitar su recurrencia [4].

El proyecto CAMbio es una fuente de lecciones aprendidas en el cambio de la seguridad de la información, algunas de las cuales se detallan a continuación:

1 *Implementación de buenas prácticas.* En el proceso de diagnóstico del estado actual de la seguridad de la información de una alcaldía de categoría 1 y su correspondiente implementación de mejoras con las acciones correctivas, se pudo constatar que al implementar las buenas prácticas sugeridas por el proceso de verificación de cumplimiento de la Norma ISO/IEC 27001, se obtuvo un efecto positivo en el fortalecimiento de la seguridad de la información en una alcaldía de categoría 1 [2, p. 20].

Este efecto se manifiesta en el avance en cumplimiento de controles general de cerca de 10 puntos porcentuales al pasar de 35,32 % a 44,92 %, lo cual representa en la escala definida un nivel Medio. De igual forma, con la aplicación de las mejoras se detectó, a nivel general, que cinco (5) dominios tuvieron un aumento en sus porcentajes de cumplimiento. Este comportamiento se aprecia en la tabla 1 y en la figura 1.

No se alcanza el nivel aceptable. Se identificó, en forma clara y concisa, que ninguno de los dominios alcanza un nivel Aceptable ni mucho menos un nivel Objetivo, en el proceso de mejoras implementado. La figura 2 muestra que todos los dominios se encuentran por debajo de los niveles Aceptables y Objetivo.

Para alcanzar los niveles de Aceptación y de Objetivo, se deben implementar mejoras en el futuro cercano en distintas áreas: Servicios logísticos y administrativos, Gestión Humana y Gerencia de Sistemas. Estas mejoras se describen en la Tabla 2.

Riesgos a los que se expone una alcaldía de categoría 1. Una de las grandes lecciones que se generó por medio del proyecto de seguridad de la información en la Alcaldía fue descubrir los primeros indicios de las vulnerabilidades y

Tabla 1. Porcentaje de mejoras de los dominios

Dominio	Descripción	% de cumplimiento		
		Diagnóstico	Mejora	Observación
A5	Política de seguridad	27,78	61,11	Aumentó
A6	Seguridad organizacional	28,45	28,45	Igual
A7	Gestión de activos	0,00	15,00	Aumentó
A8	Seguridad del recurso humano	22,22	22,22	Igual
A9	Seguridad física y ambiental	54,40	54,40	Igual
A10	Gestión de comunicaciones y operaciones	44,99	57,96	Aumentó
A11	Control de acceso	47,05	72,67	Aumentó
A12	Adquisición desarrollo y mantenimiento de los sistemas de información	46,18	46,18	Igual
A13	Gestión de incidentes de la seguridad de la información	0,00	16,00	Aumentó
A14	Aspectos de seguridad de la información en la gestión de la continuidad del negocio	0,00	0,00	Igual
A15	Cumplimiento	6,67	6,67	Igual

Fuente: Adaptado de [5, p. 5]

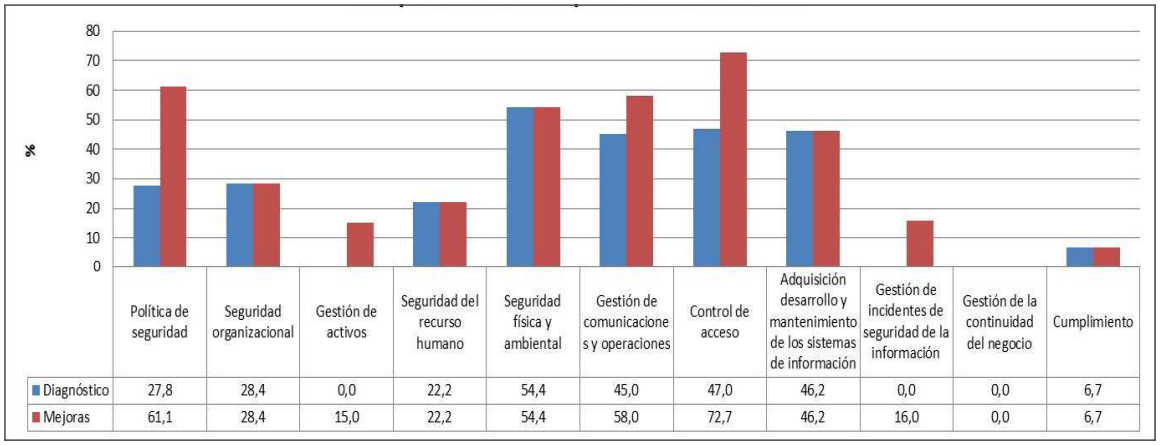
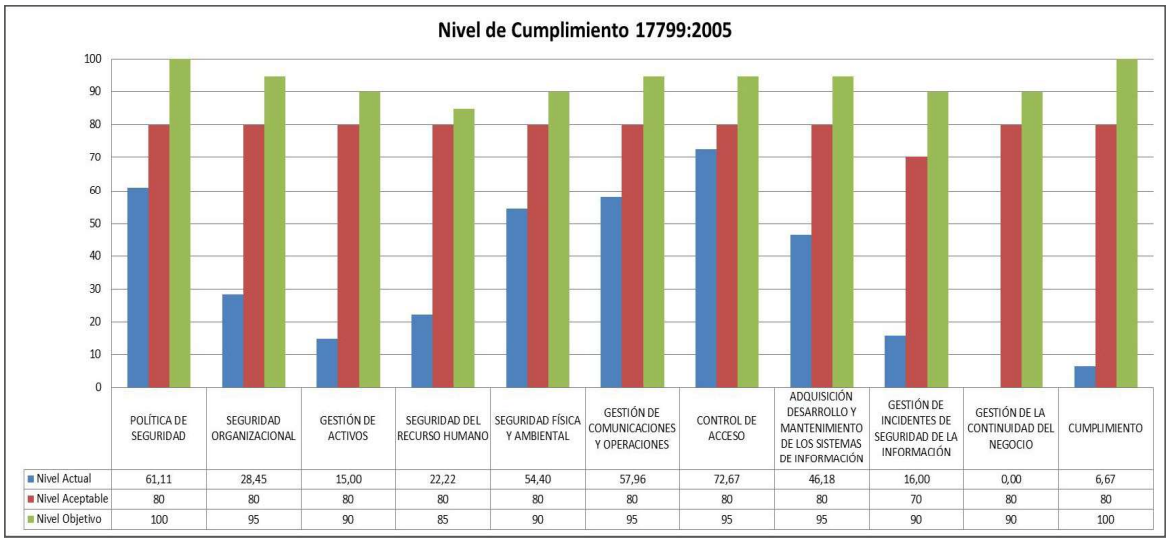


Figura 1. Comparación de avance de cumplimiento de la norma entre el diagnóstico y la mejora por dominios.
Fuente: Adaptado de (5, p. 5)



	POLÍTICA DE SEGURIDAD	SEGURIDAD ORGANIZACIONAL	GESTIÓN DE ACTIVOS	SEGURIDAD DEL RECURSO HUMANO	SEGURIDAD FÍSICA Y AMBIENTAL	GESTIÓN DE COMUNICACIONES Y OPERACIONES	CONTROL DE ACCESO	ADQUISICIÓN DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	CUMPLIMIENTO
Nivel Actual	61,11	28,45	15,00	22,22	54,40	57,96	72,67	46,18	16,00	0,00	6,67
Nivel Aceptable	80	80	80	80	80	80	80	80	70	80	80
Nivel Objetivo	100	95	90	85	90	95	95	95	90	90	100

Figura 2. Niveles de cumplimiento con respecto al nivel aceptable y al nivel objetivo.
Fuente: Adaptado de (6, p. 20)

Tabla 2. Mejoras a ser implementadas en el futuro cercano

Área	Mejoras a implementar
Servicios Logísticos y Administrativos	• Contar con un sistema de control de acceso físico biométrico. • Contar con una central de monitoreo de control de acceso físico.
Gestión Humana	• Utilización de una plataforma virtual para gestión de inducción, capacitación y consulta. • Utilización de una plataforma virtual para gestión de desempeños y otros indicadores. • Planteamiento como un proyecto de desarrollo tecnológico a cargo de la oficina de Modernización. • Utilización de un Ambiente Educativo Virtual, como por ejemplo Moodle.
Gerencia de Sistemas	• Continuar el proceso de establecimiento de SGSI. • Iniciar la implementación de los procesos de Planes de contingencia en informática (ISO/IEC 27001 A14 – GTC 176) y de Gestión de incidentes (ISO/IEC 27001 A13 – GTC 169)

Fuente: Adaptado de (7, p. 7)

amenazas que conforman los riesgos de la información a los que se expone una alcaldía de categoría 1. A continuación, se presenta un resumen de estos riesgos [7, p. 8]:

- Los datos y la información que se recogen, analizan, almacenados, comunicados y reportados, pueden ser objeto de robo, mal uso, pérdida y corrupción.
- Los datos y la información pueden ponerse en peligro por la mala educación y la formación, el uso indebido y el incumplimiento de los controles de seguridad.
- Incidentes de seguridad de la información pueden originar pérdida de prestigio y desconfianza, pérdida financiera, incumplimiento de las normas y la legislación, así como posibles demandas judiciales impuestos en contra de la Alcaldía.

Acciones para controlar los riesgos. Una alcaldía de categoría 1 deberá determinar cuáles son las acciones que le permitirán mitigar los riesgos identificados, por ello llevará a cabo las evaluaciones de riesgos para reconocer, cuantificar y priorizar los riesgos.

Los controles serán seleccionados e implementados para mitigar los riesgos identificados. Las evaluaciones del riesgo se harán mediante un enfoque sistemático para identificar y estimar la magnitud de los riesgos.

Política de uso aceptable de extranet segura. En el proyecto se determinó que una alcaldía de categoría 1 debe usar buenas prácticas de uso aceptable de extranet segura, ya que la extranet contiene información confidencial que puede estar en peligro si los usuarios no siguen estas buenas prácticas.

Además, los empleados de una alcaldía de categoría 1 estarán obligados a tener acceso a los recursos brindados por medio de la extranet para que puedan llevar a cabo sus funciones. Todo el personal que tenga acceso, en forma segura, a la extranet en cualquier forma, debe leer y entender la política de uso aceptable (AUP).

Política de uso aceptable de internet. Existe la posibilidad de la pérdida de productividad de los empleados, si ellos gastan demasiado tiempo navegando en internet. Por tal razón, las buenas prácticas de la política de uso aceptable de internet pretenden garantizar el uso efectivo del tiempo laboral, evitando el uso ilegal o inapropiado de internet.

Política de uso aceptable de correo electrónico. Las buenas prácticas de la política de uso aceptable de correo electrónico pretenden garantizar el uso efectivo del tiempo laboral, evitando así el uso ilegal o inapropiado del correo electrónico. En especial:

- Los correos electrónicos pueden contener contenido inadecuado que no debe ser visto por los usuarios.
- Los correos electrónicos pueden contener códigos maliciosos, los cuales podrían acceder o dañar los datos o reenviar datos confidenciales a un tercero.
- También existe la posibilidad de la pérdida de productividad de los empleados, si ellos gastan demasiado tiempo enviando y recibiendo correos electrónicos.

Política de creación de copias de seguridad. El objetivo de las buenas prácticas de creación y mantenimiento de copias de seguridad es el de asegurarse de que siempre es posible recuperar la información y el software en una alcaldía de categoría 1, ante los siguientes acontecimientos:

- La información puede perderse como resultado de accidentes en dispositivos de almacenamiento, eliminación o corrupción de información.
- La integridad y disponibilidad de la información crítica debe ser mantenida mediante la realización de copias regulares a otros medios.

Política de control de acceso. Las buenas prácticas orientadas al control del acceso a la información en una alcaldía de categoría 1 tienen como objeto su protección contra la divulgación, modificación o destrucción (accidental o maliciosa), mediante el control de quien tiene los derechos de uso de los diferentes recursos de información y de protección contra el uso no autorizado. Lo anterior como contramedida para mitigar los siguientes riesgos:

- Existe la posibilidad de que en ocasiones la información crítica puede ser divulgada o accedida accidental o ilegalmente por usuarios sin la debida autorización. Con esto se puede dar el caso que esta información sea borrada o tomarla como base para hacer fraudes o para dañar el buen nombre. Esta política está destinada a mitigar ese riesgo.
- No tener buenas prácticas en el control de acceso puede tener un efecto negativo, muy significativo, sobre el funcionamiento eficaz de una alcaldía de categoría 1 y podría resultar en pérdidas financieras y la incapacidad para proporcionar los servicios necesarios al ciudadano.

Política de autorización del usuario, identificación y autenticación. La pérdida de control de acceso de la información ocasiona que esta pueda ser divulgada o accedida por usuarios sin la debida autorización, y al tener acceso, dicha información puede ser borrada o tomada como base para cometer fraudes o para dañar el buen nombre de una alcaldía de categoría 1. Se hace necesario el uso de los controles de au-

torización, identificación y autenticación para garantizar que sólo los usuarios autorizados utilicen los sistemas de información.

Sin los debidos controles de autorización, identificación y autenticación, existe la posibilidad de que los sistemas de información sean accesados ilícitamente y que la seguridad de los sistemas de información sea comprometida.

Política de escritorio y pantalla limpia. Las buenas prácticas de escritorio y pantalla limpia reducen el riesgo de accesos no autorizados de la información, asimismo también se reduce el riesgo de pérdida o daño de la información fuera del horario de trabajo normal. Adicionalmente, los medios de almacenamiento de la información utilizados en una política de escritorio y pantalla limpia podrían proteger dicha información contra desastres como fuego, terremotos, inundaciones o explosiones.

El propósito de esta política es establecer una cultura de seguridad en todos los empleados en una alcaldía de categoría 1 acerca de la importancia del escritorio limpio. Además, las razones principales para implementar buenas prácticas de escritorio limpio son:

- Un escritorio limpio puede producir una imagen positiva ante los visitantes.
- Reduce la amenaza de un incidente de seguridad. Por ejemplo, cuando la oficina se encuentra desatendida puede accederse a información confidencial por personal no autorizado.
- Los documentos sensibles que quedan al descubierto pueden ser sustraídos o alterados.

Política aseguramiento (*hardening*) de infraestructura. Sin un eficaz aseguramiento de infraestructura, hay un aumento del riesgo de no contar con la disponibilidad de los sistemas. Esto puede ser causado por atacantes, virus y programas maliciosos que explotan las vulnerabilidades de los sistemas.

Las buenas prácticas son fundamentadas en que la mayoría de los sistemas realiza un número limitado de funciones. Por ello, es posible reducir el número de posibles vectores de ataque con la eliminación de software innecesario, de cuentas de usuario que no se usen o de servicios que no son requeridos ni planificados entre las funciones del sistema.

Política gestión vulnerabilidad técnica y de parches. El objetivo de la gestión de vulnerabilidad y de parches es mantener los componentes que forman parte de la infraestructura de tecnología de la información (*hardware, software* y servicios) al día con los últimos parches y actualizaciones.

La gestión de vulnerabilidad y de parches es una parte importante porque buscar mantener los componentes de la infraestructura de tecnología de la información a disposición del usuario final. Sin pruebas de vulnerabilidad y de parches, la infraestructura de tecnología de la información podría caer en problemas, que pueden corregirse con la actualización periódica del *software, firmware* y controladores. Por su parte, un parcheo deficiente puede permitir que los virus y el *spyware* infecten la red y facilitar que las debilidades de seguridad puedan ser explotadas.

Política de procedimiento de reporte de incidentes. Los incidentes de seguridad de la información deben ser reportados inmediatamente para permitir que el problema sea investigado y resuelto y para reducir el riesgo si se repite. Por ello, es de vital importancia tener un procedimiento para reportar un incidente de seguridad informática.

III. CONCLUSIONES

En el proyecto en Seguridad de la información desarrollado en una alcaldía de Categoría 1, en convenio con el Ministerio de Tecnologías de la Información y las Comunicaciones (MiniTIC), se creó el escenario propicio, primero, para detectar las malas prácticas en el manejo y tratamiento de la información que la ponen en riesgo; y segundo, con la implementación de buenas prácticas, se apropió de lecciones aprendidas que deben (como mejor práctica)ser utilizadas para resguardar y proteger la información en la alcaldía.

Todas estas buenas prácticas, basadas en la Norma ISO/IEC 27001, que debe seguir una alcaldía de categoría 1, reposan en los documentos generados por el proyecto como lo son: el Manual de la seguridad de la información, las distintas políticas de seguridad de la información, el documento ejecución de la implementación y el documento resultado de la auditoría interna. Toda la documentación se registra en un sistema actualizable de documentos, permitiendo su consulta y seguimiento por parte de todos los involucrados en el Sistema de Gestión de Seguridad de la Información (SGSI).

IV. REFERENCIAS BIBLIOGRÁFICAS

[1] MINISTERIO de Tecnologías de la Información y las Comunicaciones (MinTic). *Manual 3.0 de gobierno en línea. Manual para la implementación de la estrategia de Gobierno en línea en las entidades del orden nacional de la República de Colombia.* Bogotá: MinTic, 2011.

[2] OFICINA DE MODERNIZACIÓN. Alcaldía de Barranquilla. *Proyecto de seguridad informática-E-001-Documento de diagnóstico inicial y oportunidades de mejora del sistema de gestión de seguridad de la información.* Barranquilla: Alcaldía de Barranquilla, 2012.

[3] LOMBARDERO, Luis (Col.) *Manual para la formación en medio ambiente.* Madrid: Bureau Veritas Formación S. A., 2008.

[4]Proyecto CAMBio. L*ecciones aprendidas. Sistema de lecciones aprendidas. Proyecto CAMBio* [en línea] 2010. [Fecha de consulta: 1 de diciembre de 2020.] Disponible en: http://www.leccionesaprendidas.org/?locale=es.

[5] OFICINA DE MODERNIZACIÓN ALCALDÍA DE BARRANQUILLA. *Proyecto de seguridad informática-E-003-Documento de comparación de análisis de cumplimiento dominios entre el diagnóstico inicial y la aplicación de mejoras.* Barranquilla: Oficina de Modernización. Alcaldía de Barranquilla, 2012.

[6] OFICINA DE MODERNIZACIÓN. ALCALDÍA DE BARRANQUILLA. *Proyecto de seguridad informática-E-002-Documento de auditoría interna SGSI después de aplicar las mejoras.* Barranquilla: Oficina de Modernización. Alcaldía de Barranquilla, 2012.

[7] OFICINA DE MODERNIZACIÓN. Alcaldía de Barranquilla. *Proyecto de seguridad informática-E-004-Documento de lecciones aprendidas.* Barranquilla: Oficina de Modernización. Alcaldía de Barranquilla, 2012.

[8] GUZMÁN, Ambar Rosa, SÁNCHEZ, Sael, GARCÍA, Eugenio. Efecto de los residuos de una industria cerámica sobre la contaminación del suelo. *Revista Ciencias Técnicas Agropecuarias* [en línea]. 2007, 16 (4), 46-52 [fecha de consulta 5 de marzo de 2020]. ISSN: 1010-2760. Disponible en: https://www.redalyc.org/articulo.oa?id=93216411

[9] MASERA, D., VILLAS, R. *APELL para minería. Guía para la industria minera a fin de promover la concientización y preparación para emergencias a nivel local* Informe Técnico N.° 41. Río de Janeiro: CETEM/CYTED/CNPq, 2004.

[10]BERREZUETA, E. y DOMÍNGUEZ, M. J. (Eds.). *Técnicas aplicadas a la caracterización y aprovechamiento de recursos geológicos - mineros.* España: Red Minería XXI, CYTED e Instituto Geológico Minero de España. 2010. ISBN: 978-84-96023-87-1.

[11] GUTIÉRREZ CONDE, M. *Operación de la presa de relaves del Proyecto Toromocho* [en línea]. Tesis (Título de Ingeniero Metalurgista. Arequipa, Perú): Universidad Nacional de San Agustín de Arequipa, 2015. Disponible en http://repositorio.unsa.edu.pe/handle/UNSA/2557

[12] ROJAS VILLANUEVA, A. *Manejo ambiental relaves - disposición subacuática.* [en línea]. Tesis (Título de Ingeniero Metalurgista. Lima, Perú): Universidad Nacional Mayor de San Marcos, 2007. Disponible en: https://hdl.handle.net/20.500.12672/2117

[13] ZÚÑIGA-SUÁREZ, A. et al. Desarrollo de ladrillos mejorados (LM) y uso de nuevas tecnologías en la fabricación de ladrillos ecológicos (LE). *En: Proceedings of the 3rd International Congress on Sustainable Cons-*

truction and Eco-Efficient Solutions. Ponencia. Sevilla: Universidad de Sevilla. Escuela Técnica Superior de Arquitectura. 2017. pp. 1194-1218. Disponible en: https://idus.us.es/handle/11441/59467

[14] BORLONE, M. *Estabilidad sísmica en presa de relave construida por el método*. [en línea]. Tesis (Título de Ingeniero Civil). 2012, Santiago de Chile: Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas. Disponible en: http://repositorio.uchile.cl/handle/2250/112569

[15] MINISTERIO DEL MEDIO AMBIENTE (Perú). Aprende a prevenir los efectos del mercurio. Módulo 2: Residuos y áreas verdes, 2016. Lima: Autor.

[16] ROJAS, Luis. *Diseño de presas de relaves*. Lima: s. n., 2002.

[17] ALMERCO, D. *Construcción de dique con tratamiento del relave, en mina Catalina Huanca – región Ayacucho* [en línea]. Tesis (Título de Ingeniero Civil). 2014, Lima (Perú): Universidad de San Martín de Porres. Facultad de Ingeniería y Arquitectura. Disponible en: https://hdl.handle.net/20.500.12727/1045

[18] ROMERO BAYLÓN, A., FLORES CHÁVEZ, S. (2010). Reuso de relaves mineros como insumo para la elaboración de agregados de construcción para fabricar ladrillos y baldosas. *Industrial Data, 13*(2), 75-82. https://doi.org/10.15381/idata.v13i2.6193

[19] ICONTEC. Sistema de Gestión de la Seguridad de la Información (SGSI). 2011. p. 332. ISBN-10: 9589383939.

[20] ALEXANDER, Alberto. *Diseño de un sistema de gestion de seguridad de informacion. Óptica ISo 27001:2005*. Bogotá: Alfa Omega editores, 2007. p. 176. ISBN: 978-958-682-713-3