

**FACULTAD DE INGENIERÍA**

**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

**GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN**

**Autor(es):**

Ramos Curi, Jacob

Rodríguez Mayta, Gianmarco (https://orcid.org/0000-0001-6849-5140)

Rodríguez Trujillo, Axel Esteban (https://orcid.org/0000-0001-8979-2785)

Roman Machacuay, Yeltsin Fredy (https://orcid.org/0000-0003-1303-5459)

Surco Licas, Alfredo (<https://orcid.org/0000-0002-2791-4211>)

Temoche Imán, Jairo Alexis(https://orcid.org/0000-0001-6462-0848)

**Asesor:**

ING. Falcón Hilario, Francisco Manuel

**Línea de investigación:**

Gestión de Servicios de Tecnología de Información

**LIMA – PERÚ**

**DEDICATORIA**

Dedico esta investigación a Dios por guiar mi camino en mi formación profesional. Asimismo, a mis padres por haberme forjado como la persona que soy en la actualidad; muchos de mis logros se los debo a ustedes entre los que se incluye este.

**AGRADECIMIENTO**

Agradezco a Dios por permitirme seguir superándome. A mi maestro HILARIO FALCON, FRANCISCO MANUEL por guiarnos en la elaboración de este trabajo de investigación al contribuir con su experiencia.

**INTRODUCCIÓN**

La seguridad informática es un tema al que mucha gente no le da la importancia que realmente tiene; muchas veces por el hecho de considerar que es inútil o que jamás la utilizara. Pero en el mundo moderno, cada día más y más personas mal intencionadas intentan tener acceso a los datos de nuestros ordenadores. La seguridad es un factor imprescindible en todos los ámbitos profesionales y en la informática, es especialmente importante porque en los ordenadores es donde está almacenada la información confidencial de una empresa o de cualquier otro particular.

Es importante porque muchas empresas son amenazadas constantemente en sus activos lo que pudiera representar miles o millones de Soles en pérdidas. Las vulnerabilidades en los sistemas de información pueden representar problemas graves, por ello es muy importante comprender los conceptos necesarios para combatirlos y defender los posibles ataques a la información.

El acceso no autorizado a una red informática o a los equipos que en ella se encuentran puede ocasionar en la gran mayoría de los casos graves problemas. Uno de las posibles consecuencias de una intrusión es la pérdida de datos. Es un hecho frecuente y ocasiona muchos trastornos, sobre todo si no estamos al día de las copias de seguridad. Y aunque estemos al día, no siempre es posible recuperar la totalidad de los datos.

Otro de los problemas más dañinos es el robo de información sensible y confidencial. La divulgación de la información que posee una empresa sobre sus clientes puede acarrear demandas millonarias contra esta, o un ejemplo más cercano a usted es el de nuestras contraseñas de las cuentas de correo por las que intercambiamos información con otros.

Hoy día es común ver como cada vez se está siendo más dependientes de las computadoras como herramienta indispensable. Ya no es extraño ver que una gran parte de la población tiene acceso a este tipo de dispositivos informáticos, ni tampoco es el hecho de que puedan tener acceso a la red de redes, que es el Internet. También, muchas de las actividades que solían hacerse manualmente, ahora pueden hacerse a través de medios informáticos, lo cual es una gran ventaja, pues ahorra tiempo, y dinero la mayoría de las veces. Pero, así como se puede aprovechar la tecnología para cosas buenas, también se pueden aprovechar para cometer delitos. Por lo tanto, en la actualidad es común ver que se cometen una gran cantidad de delitos en los que se ve involucrado algún sistema de cómputo ya sea como medio, o fin. Por ese motivo me ayudará a usted en la medida de lo posible, a darle las herramientas para que pueda defenderse contra la pérdida de datos o el robo de información de una mejor manera.

Pero antes, tengo que hacer inca pie en algo importante: Mantener un sistema informático o una red informática libre de intrusiones no es tarea fácil. Hay que actuar siempre con precaución y siguiendo unas normas básicas para evitar daños.

Recuerde, la seguridad es inversamente proporcional a la comodidad. Si desea un sistema seguro deberá esforzarse por ello, emplear contraseñas fuertes y diferentes y seguir todo un procedimiento para mantener el sistema.

**2. DESARROLLO**

Controles de seguridad del ISMS

Los controles de seguridad del ISMS abarcan múltiples dominios de seguridad de la información, como se especifica en la norma ISO 27001. El catálogo contiene directrices prácticas con los siguientes objetivos:

* **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**. Una dirección y un apoyo general ayudan a establecer políticas de seguridad adecuadas. La política de seguridad es única para su empresa, concebida en el contexto de sus cambiantes necesidades empresariales y de seguridad.
* **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.** Aborda las amenazas y los riesgos dentro de la red corporativa, incluidos los ciberataques de entidades externas, las amenazas internas, los fallos del sistema y la pérdida de datos.
* **GESTIÓN DE ACTIVOS.** Este componente abarca los activos de la organización dentro y fuera de la red informática de la empresa, lo que puede implicar el intercambio de información empresarial sensible.
* **SEGURIDAD DE LOS RECURSOS HUMANOS**. Políticas y controles relativos a su personal, actividades y errores humanos, incluyendo medidas para reducir el riesgo de amenazas internas y capacitación de la fuerza laboral para reducir lapsos de seguridad no intencionales.
* **SEGURIDAD FÍSICA Y AMBIENTAL**. Estas directrices cubren las medidas de seguridad para proteger el hardware físico de TI de daños, pérdidas o accesos no autorizados. Si bien muchas organizaciones están aprovechando la transformación digital y manteniendo la información confidencial en redes de nubes seguras fuera de las instalaciones, debe considerarse la seguridad de los dispositivos físicos utilizados para acceder a esa información.
* **GESTIÓN DE LAS COMUNICACIONES Y LAS OPERACIONES.** Los sistemas deben funcionar respetando y manteniendo las políticas y controles de seguridad. Las operaciones diarias de TI, como el suministro de servicios y la gestión de problemas, deben seguir las políticas de seguridad de TI y los controles del SGSI.
* **CONTROL DE ACCESO**. Este dominio de políticas se ocupa de limitar el acceso al personal autorizado y de controlar el tráfico de la red para detectar comportamientos anómalos. Los permisos de acceso se relacionan con los medios digitales y físicos de la tecnología. Las funciones y responsabilidades de los individuos deben estar bien definidas, y el acceso a la información empresarial solo debe estar disponible cuando sea necesario.
* **ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.** Las mejores prácticas de seguridad deben mantenerse a lo largo de todo el ciclo de vida del sistema informático, incluidas las fases de adquisición, desarrollo y mantenimiento.
* **SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE INCIDENTES**. Identificar y resolver los problemas de la TI de manera que se minimice el impacto para los usuarios finales. En entornos de infraestructura de red complejos, pueden requerir soluciones tecnológicas avanzadas para identificar métricas de incidentes perspicaces y mitigar proactivamente los posibles problemas.
* **GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.** Evitar las interrupciones de los procesos comerciales siempre que sea posible. Lo ideal sería que cualquier situación de desastre fuera seguida inmediatamente por la recuperación y los procedimientos para minimizar los daños.
* **CUMPLIMIENTO.** Los requisitos de seguridad deben ser aplicados por los organismos reguladores.
* **CRIPTOGRAFÍA.** Entre los controles más importantes y eficaces para proteger la información sensible, no es una bala de plata por sí sola. Por lo tanto, el ISMS rige la forma en que se aplican y gestionan los controles criptográficos.
* **RELACIONES CON LOS PROVEEDORES.** Es posible que los proveedores y los socios comerciales de terceros necesiten acceder a la red y a los datos sensibles de los clientes. Puede que no sea posible aplicar controles de seguridad a algunos proveedores. Sin embargo, deben adoptarse controles adecuados para mitigar los posibles riesgos mediante políticas de seguridad de la tecnología de la información y obligaciones contractuales.

**MEJORA CONTINUA DE LA SEGURIDAD DE LA INFORMACIÓN**

* **PLANIFICAR.** Identificar los problemas y recopilar información útil para evaluar el riesgo de seguridad. Definir las políticas y procesos que pueden utilizarse para abordar las causas fundamentales de los problemas. Desarrollar métodos para establecer una mejora continua de las capacidades de gestión de la seguridad de la información.
* **HACER.** Aplicar las políticas y procedimientos de seguridad concebidos. La implementación sigue las normas ISO, pero la implementación real se basa en los recursos disponibles de su empresa.
* **VERIFICAR**. Supervisar la eficacia de las políticas y controles del ISMS. Evaluar los resultados tangibles así ́ como los aspectos de comportamiento asociados a los procesos del SGSI.
* **ACTUAR**. Concéntrese en la mejora continua. Documentar los resultados, compartir el conocimiento y usar un circuito de retroalimentación para abordar futuras iteraciones del modelo PCDA de implementación de políticas y controles del ISMS.

**Los peligros pueden corresponder a cuatro categorías básicas:**

Entre los desastres más comunes que pueden afectar un sistema de computación, se encuentran:

* Virus.
* Fuego.
* Filtraciones e inundaciones.
* Cortes de [electricidad](https://www.monografias.com/trabajos10/nofu/nofu.shtml) y fluctuaciones en el suministro.
* Interferencia de [fuentes](https://www.monografias.com/trabajos10/formulac/formulac.shtml#FUNC) eléctricas externas.
* Cortes de [gas](https://www.monografias.com/trabajos10/gase/gase.shtml), [agua](https://www.monografias.com/trabajos14/problemadelagua/problemadelagua.shtml) y otros [servicios](https://www.monografias.com/trabajos14/verific-servicios/verific-servicios.shtml) públicos.
* Fallas mecánicas.
* Sabotaje.
* Empleados descontentos.
* Uso indebido de recursos.

**VULNERABILIDAD**

Es la debilidad que presenta una organización frente a las contingencias latentes que tienen lugar en el entorno del [procesamiento de datos](https://www.monografias.com/trabajos14/datos/datos.shtml#pro). Dada una contingencia, la vulnerabilidad es la falta de protección frente a ella. Las siguientes listas señalan las distintas formas en las que una organización contribuye con un grado de mayor o menor negligencia a que se concreten peligros latentes. También en un sistema informático lo que queremos proteger son sus activos, es decir, los recursos que forman parte del sistema y que podemos agrupar en:

* Hardware: elementos físicos del sistema informático, tales como [procesadores](https://www.monografias.com/trabajos5/sisope/sisope.shtml), [electrónica](https://www.monografias.com/trabajos5/electro/electro.shtml) y cableado de red, medios de almacenamiento (cabinas, discos, cintas, [DVD](https://www.monografias.com/trabajos16/dvd-video-digital/dvd-video-digital.shtml)).
* Software: elementos lógicos o programas que se ejecutan sobre el hardware, tanto si es el propio sistema operativo como las aplicaciones.
* Datos: comprenden la información [lógica](https://www.monografias.com/trabajos15/logica-metodologia/logica-metodologia.shtml) que procesa el software haciendo uso del hardware. En general serán informaciones estructuradas en bases de datos o paquetes de información que viajan por la red.
* Otros: fungibles, personas, infraestructuras. Aquellos que se 'usan y gastan' como puede ser la tinta y papel en las [impresoras](https://www.monografias.com/trabajos11/trimpres/trimpres.shtml), los soportes tipo DVD o incluso cintas si las copias se hacen en ese medio, etc.

Incluso de todos ellos, el activo más crítico son los datos. El resto se puede reponer con facilidad y los datos. Sabemos que dependen de que [la empresa](https://www.monografias.com/trabajos11/empre/empre.shtml) tenga una buena [política](https://www.monografias.com/Politica/index.shtml) de copias de seguridad y sea capaz de ponerlos en el estado más próximo al momento en que se produjo la pérdida. Esto puede suponer para la empresa, por ejemplo, la dificultad o imposibilidad de reponer dichos datos con lo que conlleva pérdida de tiempo y dinero.

**CONSECUENCIA**

Una consecuencia es el daño o la pérdida que [la organización](https://www.monografias.com/trabajos6/napro/napro.shtml) sufriría ante la ocurrencia de una contingencia. Las consecuencias pueden ser de diverso tipo y grado y afectar a cualquiera de los recursos informáticos (datos, equipo, personas, software e instalaciones). Algunas de las consecuencias más importantes que pueden darse en forma inmediata son:

* Imposibilidad de procesar.
* Pérdida de archivos.
* Pérdida de [registros](https://www.monografias.com/trabajos7/regi/regi.shtml).
* Modificación de registros.
* Lectura indebida/divulgación.
* Uso indebido de recursos.

También existen otras consecuencias, cuyas manifestaciones pueden calificarse de mediatas:

* Legales o regulatorias.
* Económicas o financieras.
* Cambios en la relación con los clientes, [proveedores](https://www.monografias.com/trabajos6/lacali/lacali.shtml#influencia) o el público.
* Incidencia en otros sistemas.

Las consecuencias tienen una expresión monetaria que está dada por el recurso informático afectado y por el impacto que dicha situación crea sobre la operación de la empresa, incluyendo el lucro cesante. La estimación monetaria de las pérdidas que puede generar cada una de las contingencias es una etapa importante de la [evaluación](https://www.monografias.com/trabajos11/conce/conce.shtml) de la seguridad.

**MAYOR RIESGO**

* Beneficio personal
* Síndrome de Robín Hood
* Odio a la organización
* Mentalidad turbada
* Equivocación de ego
* Deshonestidad del departamento
* Problemas financieros de algún individuo
* Fácil modo de desfalco

**CONCLUSIONES**

La seguridad de la información es un aspecto, que debe ser parte de la cultura organizacional, inherente a toda actividad humana; cursos, seminarios, y talleres no bastan, hay que interiorizar en las personas de la organización, la necesidad y beneficios de dicha cultura, así como los riesgos de no tenerla.

Su principal objetivo es la protección de los reactivos informáticos del usuario. Además de que debemos proteger y cómo podemos realizar esta actividad para mantener asegurados nuestros archivos sean importantes o no, ya que son de uso exclusivo del usuario.

Es fundamental la participación de la alta dirección de la empresa, porque ellos son los principales interesados en que su proceso de exportación cumpla con las medidas de seguridad que exige el BASC para sus miembros.

Se deduce que por más que se realice la implementación del SGSI no se puede garantizar el 100% de la seguridad, dado que el propósito del SGSI es gestionar los riesgos de la información, es decir que sean conocidos, gestionados y minimizados.

Podemos comprender que cualquier empresa que implemente el sistema de gestión de riesgos de la información, cumplirá con los estándares internacionales y certifica sus procesos de seguridad dado que identifica, gestiona y minimiza los riesgos que posee la seguridad de la información.

Por último, destacamos que la seguridad de la información es un aspecto, que debe ser parte de la cultura organizacional, inherente a toda actividad humana; cursos, seminarios, y talleres no bastan, hay que interiorizar en las personas de la organización, la necesidad y beneficios de dicha cultura, así como los riesgos de no tenerla.

REFERENCIAS BIBLIOGRÁFICAS

CÁRDENAS-SOLANO, Leidy-Johanna; MARTÍNEZ-ARDILA, Hugo; BECERRA-ARDILA, Luis-Eduardo. Gestión de seguridad de la información: revisión bibliográfica. *El profesional de la información (EPI)*, 2016, vol. 25, no 6, p. 931-948.

MERINO VÁSQUEZ, José Christiam; TORRES ASENCIOS, Edgar Junior. Implementación de un modelo de la seguridad de la información basados en ITIL v3 para una Pyme de TI. 2016.

CLAUDIA VICTORIA ALVARADO (2021) Sistema de gestión de seguridad de la información: qué es y sus etapas. Disponible en: <https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas>

VALENCIA-DUQUE, Francisco Javier; OROZCO-ALZATE, Mauricio. Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 2017, no 22, p. 73.

MERO GARCÍA, Alejandro Fabián. *Implantación de un sistema de gestión de seguridad de información (SGSI) en el distrito de salud 13d04 24 de mayo–Santa Ana–Olmedo–salud de la provincia de Manabí*. 2016. Tesis de Maestría. PUCE.

ESPINOSA BETANCUR, Juan Guillermo, et al. Sistema de gestión de seguridad de la información para los tres procesos misionales de la corporación autónoma regional de risaralda (CARDER). 2016.

RIAÑO-CASALLAS, Martha Isabel; HOYOS NAVARRETE, Eduardo; VALERO PACHECO, Ivonne. Evolución de un sistema de gestión de seguridad y salud en el trabajo e impacto en la accidentalidad laboral: Estudio de caso en empresas del sector petroquímico en Colombia. *Ciencia & trabajo*, 2016, vol. 18, no 55, p. 68-72.

SIERRA ORTIZ, Sandra Milena, et al. Diseño de sistema de gestión de seguridad de la información en Saludvida EPS.

Mantilla Guerra, Aníbal Ruben. 2018. Gestión de seguridad de la información con la norma ISO:27001:2013. Disponible en: <https://www.revistaespacios.com/a18v39n18/a18v39n18p05.pdf>

POICON, RAMIREZ. 2020. Propuesta de un sistema de gestión de seguridad de la información para la Municipalidad Distrital de Marcavelica, mediante la NTP- ISO/IEC 27001:2014. Disponible en: <https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/58301/Paicon_ZJMA-Ram%c3%adrez_MO-SD.pdf?sequence=1&isAllowed=y>

Agurto Castillo, Manuel Armando. 2017. Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001. Piura: Universidad César Vallejo, 2017.

Castro Siguas, Joshimar Japhet. 2018. Implementación de la NTP ISO/IEC 27001:2014 para mejorar la gestión de la seguridad en los sistemas de información de la Autoridad Portuaria Nacional, Callao - 2017. Lima, Perú : Universidad Autónoma del Perú, 2018.

CHUNA CHINGA, Gerson Isaac Luciano. 2018. Propuesta de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para la DRTPE - filial Piura”. Piura : Universidad César Vallejo, 2018

Ayala , M. (2017). Sistema de gestión de seguridad de información Para mejorar el proceso de gestión del riesgo En un hospital nacional, 2017. Tesis, Universidad César Vallejo, Lima Perú

Mera. A. (2014). Diseño del modelo de gestión de seguridad de la información del sistema ERP de EP PETROECUADOR de acuerdo a norma ISO/IEC 27002 y COBIT 5. (Tesis de Maestría). Universidad. Ecuador. Recuperado de:http://repositorio.espe.edu.ec/bitstream/21000/8073/1/T-ESPE047641.pdf

Juan David Pedroza Arango (2016) IMPLEMENTACION DE UN GESTOR DE SEGURIDAD DE LA INFORMACION Y GESTION DE EVENTOS (SIEM. Universidad de San Buenaventura. Medellín 2016. Disponible en: <http://bibliotecadigital.usb.edu.co/bitstream/10819/3944/1/Implementacion_Gestor_Seguridad_Pedroza_2016.pdf>

Cao Avellaneda, Javier (14 de febrero de 2011). «Medición de un SGSI: diseñando el cuadro de mandos INCIBE. Archivado desde el original el 10 de marzo de 2020. Consultado el 9 de marzo de 2020. «Uno de los grandes beneficios de implantar un sistema de gestión basado en ISO 27001 debe ser pasar de una “seguridad basada en sensaciones” a una “seguridad

Romero Castro, M. I. y Figueroa Moràn, G. L. (2018). INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES (2a ed.). 3Ciencias. (Trabajo original publicado en 2018)