FACULTAD DE ARQUITECTURA E INGENIERÍA

Trabajo de fin de Carrera titulado:

DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27002:2013, PARA EL SISTEMA DE BOTONES DE SEGURIDAD DEL MINISTERIO DEL INTERIOR

Realizado por:

Ing. Wáshington Marcelo Contero Ramos

Director del proyecto:

Msc. Christian David Pazmiño Flores

Como requisito para la obtención del título de:

MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIÓN

QUITO, marzo de 2019

DECLARACION JURAMENTADA

Yo, WÁSHINGTON MARCELO CONTERO RAMOS, con cedula de identidad 0603334038, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente

_____

WÁSHINGTON MARCELO CONTERO RAMOS

C.C.: 0603334038

DECLARACIÓN DEL DIRECTOR DE TESIS

Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

Christian David Pazmiño Flores

Magister en Gerencia de Sistemas y Tecnologías de la Información

CC: 1719252049

LOS PROFESORES INFORMANTES

Los Profesores informantes:

Ing. Verónica Rodríguez Arboleda, MBA.

Ing. Edison Estrella Mogollón, MBA

Después de revisar el trabajo presentado lo han calificado

como apto para su defensa oral ante el tribunal examinador

Ing. Verónica Rodríguez Arboleda, MBA	Ing. Edison Estrella Mogollón, MBA

Quito, marzo de 2019

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

Wáshington Marcelo Contero Ramos

CC: 0603334038

AGRADECIMIENTOS

A la Universidad Internacional SEK, al personal docente y autoridades de la Maestría en Tecnologías de la Información, por su responsabilidad, profesionalismo y compromiso en todo el proceso de formación educativa y personal, desde el inicio hasta la finalización de la carrera.

Al Ingeniero Christian Pazmiño por su gentil y valioso aporte para el desarrollo del presente proyecto.

DEDICATORIA

El siguiente proyecto está dedicado a Dios y a la Virgen Dolorosa por ser mis protectores en la vida, por haberme bendecido con salud y sabiduría y por permitirme cumplir con un objetivo más en mi vida profesional y personal.

A mis padres Wáshington y Verónica por haberme brindado todo, por inculcarme valores y principios que me ha servido durante toda la vida, por compartir conmigo los momentos de felicidad y ser mi apoyo en los momentos difíciles.

A mis hermanos Andrés, Yesenia y a mi sobrinita Kristel, quienes por su cariño, apoyo incondicional y confianza han sido la motivación para la consecución de este trabajo.

RESUMEN

El siguiente proyecto de grado tiene como objetivo principal Diseñar una Política de Seguridad de la Información, basada en la Norma ISO/IEC 27002:2013 para el Sistema de Botones de Seguridad del Ministerio del Interior, con la finalidad de establecer las directrices y normas para la correcta gestión de la seguridad de la información. Se desarrolla un análisis de la norma ISO/IEC 27002:2013, sustentándose en lo expuesto en el EGSI (Esquema Gubernamental de Seguridad de la información), en el cual se indica que este esquema no reemplaza a la norma ISO/IEC 27002 y que, de acuerdo a las necesidades de cada institución pública, dirección o departamento, se puede definir políticas de seguridad amplias o específicas. Luego de haber realizado el levantamiento de la información de la situación actual de este sistema de seguridad integral, con los resultados obtenidos y mediante la aplicación de la metodología Magerit se determina y valora los activos, posteriormente las amenazas que puedan presentarse y finalmente se estima el impacto y los riesgos a los cuales está expuesta la información. A través de la norma NTE INEN ISO/IEC 27002:2013 se selecciona las salvaguardas o controles necesarios y más adecuados que se aplica en el desarrollo de la política de seguridad de la información. Esta política contiene características recomendadas en la norma NTE INEN ISO/IEC 27002:2013, además se incluye las definiciones, terminología, abreviaturas y responsabilidades, con el objetivo de que su aprobación y aplicación se lo pueda realizar en un corto plazo en dicha Cartera de Estado.

Palabras Clave: Política de seguridad, Metodología Magerit, Norma NTE ISO/IEC 27002:2013

ABSTRACT

The main objective of the following degree project is to Design an Information Security Policy, based on the ISO / IEC 27002: 2013 Standard for the Security Button System of the Ministry of the Interior, with the purpose of establishing the guidelines and rules for the correct management of information security. An analysis of ISO / IEC 27002: 2013 is developed, based on what is stated in the EGSI (Government Information Security Scheme), which indicates that this scheme does not replace ISO / IEC 27002 and that , according to the needs of each public institution, address or department, you can define broad or specific security policies. After having carried out the survey of the current situation of this comprehensive security system, with the results obtained and through the application of the Magerit methodology, the assets are determined and valued, subsequently the threats that may arise and finally the impact and the risks to which the information is exposed. Through the NTE INEN ISO / IEC 27002: 2013 standard, the necessary and most appropriate safeguards or controls applied in the development of the information security policy are selected. This policy contains characteristics recommended in the NTE INEN ISO / IEC 27002: 2013 standard, as well as definitions, terminology, abbreviations and responsibilities, with the aim that its approval and application can be done in a short term in said Portfolio State.

Keywords: Security politic, Magerit methodology, INEN ISO/IEC 27002:2013 standart

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

INTRODUCCIÓN

1.1. EL PROBLEMA DE INVESTIGACIÓN

1.1.1. PLANTEAMIENTO DEL PROBLEMA

El desarrollo constante y acelerado de las tecnologías de la información ha traído consigo varios problemas, la principal preocupación se centra en la manera y forma de protección de datos, principalmente de la protección de la información confidencial y sensible; que hoy en día es considerada como uno de los activos más preciados en una organización o empresa.

Los servicios tecnológicos de las instituciones y organismos públicos en el Ecuador, no han estado exentos a los problemas de seguridad de la información, un ejemplo es el Servicio de Contratación Pública, cuando su portal web fue vulnerado, por una banda que utilizaba software para adulterar datos en beneficio de empresas o personas que pagaban altas sumas de dinero, con la finalidad de obtener contratos con el Estado (El Comercio, 2015).

El grupo de activistas informáticos Anonymus, según los datos proporcionados por seguridadydefensa.com.ec; publicó información de 45000 policías, luego de realizar un ataque a una base de datos de la Policía Nacional en el año 2011 (Infobae, 2011).

De acuerdo a la información proporcionada por la Coordinación de Tecnologías de la Información del Ministerio del Interior, el Sistema de Botones de Seguridad, almacena información sensible y confidencial, la misma que es administrable y accesible desde diferentes

instancias; sin embargo la falta de procedimientos y controles en la asignación de perfiles y cuentas de usuario, administración de servicios y demás procesos internos, la hace vulnerable ante amenazas que puedan afectar a la seguridad de la información.

1.1.1.1.DIAGNÓSTICO

El Sistema de Botones de Seguridad es un Sistema Integral de Seguridad compuesto por una plataforma tecnológica, una unidad técnica – administrativa, una unidad de coordinación y la unidad de operación, enmarcados bajo los lineamientos de la Coordinación de Tecnologías de la Información del Ministerio del Interior en coordinación con la Policía Nacional.

A través de este sistema integral, se brinda un servicio de seguridad a la ciudadanía; las personas registran sus domicilios o locales comerciales en la Unidad de Policía Comunitaria (UPC) más cercana; en el caso de presentarse alguna emergencia, el ciudadano a través de su teléfono celular o convencional genera una alerta, la misma que es recibida en forma de alarma en un sistema web en el computador de las UPC y a través de un mensaje de texto en los celulares del personal policial; la Unidad de Botones de Seguridad del Ministerio del Interior, es la responsable de la administración del Sistema Integral de Seguridad, así como la responsable de establecer las medidas y procedimientos que garanticen la operatividad de la plataforma tecnológica.

El sistema de Botones de Seguridad, no dispone de una normativa o un modelo definido, aprobado y socializado que describa los procesos de gestión relacionados a la seguridad de la información.

La información registrada en su plataforma tecnológica cuenta con más de 2 700 000 registros de ciudadanos, los servicios y aplicativos tecnológicos se encuentra en un Data Center

de una empresa proveedora de servicios tecnológicos; sin embargo, los acuerdos de confidencialidad de la información no se encuentran actualizados.

El acceso a la información disponible en la plataforma tecnológica, varía dependiendo de los perfiles y tipos de usuario, las reglas y procedimientos para la asignación y renovaciones de cuenta, así como definición de privilegios, no se encuentran documentados, tampoco existe un procedimiento definido para la entrega de información.

Con la finalidad de garantizar la disponibilidad de los servicios de la plataforma tecnológica, existen SLA o Acuerdos de Nivel de Información establecidos con la empresa proveedora de servicios tecnológicos, pero a nivel interno no se encuentran documentados los procedimientos que permitan actuar en caso de incidentes o caídas algún servicio.

La amplia información disponible en la plataforma tecnológica, no se encuentra debidamente catalogada o categorizada entre información de libre entrega e información crítica y sensible.

Si bien existen reglas establecidas espontáneamente, las mismas no tienen la revisión del Oficial de Seguridad de la Información, no se encuentran aprobadas por la máxima autoridad y no son conocidas por todo el personal responsable del sistema; la información expuesta fue obtenida a través de entrevistas mantenidas con los funcionarios que trabajan en el Sistema de Seguridad, en relación a la autorización otorgada (Ver Anexo 1).

1.1.1.2. PRONÓSTICO

El Sistema de Botones de Seguridad al formar parte de los servicios estratégicos de las Unidades de Policía Comunitaria (UPC), le permite al Ministerio del Interior y a la Policía Nacional, dotar a la ciudadanía de un servicio de seguridad para los domicilios y locales

comerciales, el mismo que no tiene costo; razón por lo cual es evidente el crecimiento de registros de usuarios dentro de la base de datos, así como el crecimiento en la asignación y creación de nuevas cuentas para acceso al sistema tecnológico a través de las UPC.

El no disponer de una normativa o política de seguridad de la información, puede traer consigo riegos como el desborde de la información y filtración de contenidos, los cuales pueden afectar significativamente a la operatividad de la plataforma tecnológica.

La falta de procedimientos para solventar las caídas o incidentes en la plataforma tecnológica, puede ocasionar la indisponibilidad del servicio; un problema de este tipo, debido a su criticidad, requiere ser atendido de manera urgente, pues el servicio afectaría directamente a las UPC y a la ciudadanía en la atención a las emergencias.

El no disponer de controles y procedimientos para el acceso a la información, puede traer consigo el acceso no autorizado a la información disponible en el sistema, cuya consecuencia puede ser el robo de la información confidencial, manipulación de registros almacenados y acceso en tiempo real a las emergencias o incidentes que puedan presentarse en cualquiera de las Unidades de Policía Comunitaria a nivel nacional.

1.1.1.3. CONTROL DE PRONÓSTICO

Diseñar una Política de Seguridad de la Información basada en las norma ISO 27002 permitirá establecer los controles necesarios para el aseguramiento de la información a nivel de software y hardware en la plataforma tecnológica del sistema, así como en todos los procesos ejecutados a nivel del sistema integral de seguridad.

Al no tener definido la criticidad de los componentes e información almacenada en los aplicativos o módulos tecnológicos del Sistema de Botones de Seguridad, será necesario en

primer lugar establecer una matriz de identificación de riesgos con la finalidad de enfocar los controles necesarios en las áreas o activos críticos.

Mediante la gestión de relaciones con terceros, gestión de incidentes y los planes de contingencia y continuidad del negocio, se pretende establecer los procedimientos que permitan solventar los problemas relacionados a la indisponibilidad de servicios de la plataforma tecnológica del sistema.

La administración del sistema tecnológico, custodia de la información y la asignación de responsabilidades, deberán ser establecidas con la finalidad de proteger el acceso a la información no autorizada y a la información en general a nivel de todo el sistema integral de seguridad, para garantizar su integridad, disponibilidad y confidencialidad.

1.1.2. FORMULACIÓN DEL PROBLEMA

El sistema de Botones de Seguridad del Ministerio del Interior contiene procesos críticos y sensibles, dentro de los cuales se administra información de carácter confidencial; el mal uso del sistema y una inadecuada administración en los procesos han ocasionado problemas que comprometen la seguridad, integridad y disponibilidad de la información.

1.1.3. OBJETIVO GENERAL

Diseñar una política de seguridad de la información basada en la norma ISO 27002:2013 que permita establecer las medidas necesarias para garantizar la seguridad de la información del Sistema de Botones de Seguridad del Ministerio del Interior.

1.1.4. OBJETIVOS ESPECÍFICOS

- ✓ Realizar el levantamiento de información de la situación actual del Sistema de Botones de Seguridad del Ministerio del Interior, mediante la elaboración de una matriz de riesgos, para la identificación de posibles amenazas y vulnerabilidades en la seguridad de la información.
- ✓ Analizar la norma ISO/IEC 27002:2013, mediante la selección de los controles necesarios, que permitan minimizar la materialización de los riesgos de la seguridad de la información en el Sistema de Botones de Seguridad.
- ✓ Definir la política de seguridad de la información en base a los controles seleccionados a partir de la norma ISO/IEC 27002:2013, con la finalidad fin de establecer las medidas para la protección de la información.

1.1.5. JUSTIFICACIÓN

1.1.5.1.PRÁCTICA

El constante avance de la tecnología ha ocasionado que las organizaciones y las empresas traten de aprovechar al máximo los recursos tecnológicos disponibles para el manejo y administración de la información; sin embargo, este mismo avance, trae consigo una serie de potenciales riesgos y vulnerabilidades que pueden comprometer la confidencialidad, integridad y disponibilidad de la información en los sistemas o plataformas informáticas utilizadas.

Los virus, el espionaje, ataques informáticos, intrusiones y demás delitos informáticos pueden afectar seriamente a la continuidad del giro del negocio de las organizaciones y empresas, más aún si se trata de un sistema o plataforma en donde las acciones están enfocadas a la seguridad y protección ciudadana.

El Sistema de Botones de Seguridad es la integración de varias tecnologías en un solo sistema, el cual se orienta a brindar asistencia oportuna a la ciudadanía en casos de emergencias a través de las Unidades de Policía Comunitaria (UPC), el sistema contiene información personal de los ciudadanos registrados; bajo esta consideración es necesario diseñar una Política de Seguridad de la Información, la cual permita establecer las medidas necesarias para garantizar la seguridad de la información.

1.1.5.2.METODOLÓGICA

La identificación, planeación y diseño son tres etapas que se acoplan al proyecto de investigación a desarrollarse, mediante el levantamiento y recopilación de información, se podrá conocer y evaluar la situación actual de la gestión de la seguridad de la información dentro del Sistema de Botones de Seguridad; la planeación se realizará en función del análisis de riesgos y finalmente la aplicación de controles basados en norma técnicas como la ISO/IEC 27002:2013, permitirán definir las políticas orientadas a tratar los riesgos y vulnerabilidades a los cuales esté expuesta la información.

La política de seguridad de la información permitirá normar, estandarizar y gestionar, los procesos físicos, lógicos y organizativos asociados al manejo de la información, para lo cual se utilizará la norma NTE INEC ISO/IEC 27002:2013.

1.1.6. ESTADO DEL ARTE

Sfreddo y Flores (2012) en su artículo “Seguridad de la información de archivos: el control de acceso de archivos Públicos Estatales”, mencionan que antes de elaborar medidas para garantizar la seguridad de la información, es necesario que una institución elabore un programa para el levantamiento de información. Este programa debe tener como uno de sus objetivos

principales, establecer los lineamientos y directrices para que los empleados o trabajadores faciliten el acceso a los documentos, esto con la finalidad de aportar a la etapa previa al desarrollo de una política de seguridad.

Una vez evaluada la situación de la organización, será necesario adoptar una norma para el desarrollo de la política de seguridad de la información; dada las características y aplicabilidad a cualquier tipo de empresas y organizaciones, se menciona a la norma la Norma ISO/IEC27002, como referencia para el desarrollo de políticas de seguridad de la información.

Ledezma (2015), autora del Desarrollo de políticas de seguridad de la Información basadas en las normas ISO 27002 para una Coordinación zonal del INEC; menciona que las instituciones públicas que manejan información sensible, son propensas al robo de información.

Luego de realizar un estudio de la situación actual de la organización y una vez que se detectaron problemas referentes a fuga de información, plantea la necesidad de proteger los activos de la organización, a través de una adecuada normativa, para tal efecto se propone la aplicación de Norma ISO/IEC 27002:2013, haciendo referencia a que esta norma contiene un conjunto de buenas prácticas para la gestión de la seguridad de la información y que la aplicación de la misma sería un aporte significativo para la institución.

Ladino y Villa (2014), en la Descripción de los Fundamentos de la norma ISO 27001 e ISO 27002 y su aplicación en las Organizaciones, hace mención a una encuesta realizada en Colombia por parte de la Asociación Colombiana de Ingeniería en Sistemas (ACIS), mediante la cual se concluye que la falta de apoyo de la gerencia o directiva de una organización, no pude ser una excusa para poner en marcha acciones que garanticen la seguridad de la información; si bien la inversión pude ser costosa, la materialización de la inseguridad puede ser aún mayor, este

principio es la base que motiva al desarrollo de una política de seguridad de la información con el fin de preservar la misma.

Garavito (2015) autora del Análisis y gestión del riesgo de la información en los sistemas de información misionales de una entidad del estado, enfocado en un sistema de seguridad de la información; basado en las encuestas y al levantamiento de información realizada, presenta como principales observaciones de seguridad de la información, los siguientes aspectos:

- Sistemas con protocolos no seguros
- Falta de procedimientos documentados para copias de seguridad
- Falta de capacitaciones de concientización en la seguridad de la información
- Errores en el ingreso de datos al sistema
- No existen módulos de auditoría de registro de operaciones

Una vez evaluados los riesgos, se plantea los controles necesarios para salvaguardar la integridad, disponibilidad y confidencialidad de la información; la metodología Magerit es utilizada como primer paso para el análisis de riesgos.

Contreras (2016), menciona que la Metodología de Magerit, fue una herramienta utilizada como ayuda para analizar e identificar los riesgos existentes en la Gobernación de Boyacá, además permite documentar el inventario de activos y realizar valoraciones cuantitativas sobre éstos; a través de esta herramienta fue posible evidenciar de forma clara los activos que se encuentran en riesgo a fin de poder ser tratados de forma inmediata a través de un Sistema de Gestión de Seguridad de la Información e impementación de Políticas y normativas institucionales.

Para el desarrollo de ese proyecto se realizó una observación directa, se realizaron encuestas a los funcionarios de la Dirección de Sistemas y un levantamiento de información referente a los activos tecnológicos, con la finalidad de determinar un nivel de exposición a los posibles riesgos de vulnerabilidad de la información.

CAPÍTULO II

MARCO TEÓRICO

2.1.LA SEGURIDAD DE LA INFORMACIÓN

La información es un activo para cualquier institución u organización, ya sea esta pública o privada; la falta de información o a su vez defectuosa, puede llevar a la organización a un fracaso.

Una información puede ser considerada de calidad, cuando se satisface los requerimientos de la empresa u organización, basados en sus tres propiedades:

- ✓ La integridad
- ✓ La disponibilidad
- ✓ La confidencialidad

La seguridad de la información es la disciplina que abarca los sistemas de protección física, la prevención de accidentes o la prevención de actividades desleales por parte de los empleados de una organización o empresa (Gómez, 2007, pág. 3).

El punto de inicio para establecer y mantener con garantías de éxito la seguridad de la información, es la definición de los objetivos de una manera clara y entendible, a partir de los cuales se pueden desarrollar las políticas y procedimientos que definan un marco referencial para

situar las medidas de seguridad a implantar, teniendo en cuenta los aspectos legales que rigen la seguridad del espacio físico donde se sitúa una empresa (Recio, 2012, pág. 14).

Los objetivos de la seguridad de la información, se fundamentan en los tres principios que debe cumplir un sistema informático (Rodríguez, 2016):

2.1.1. Confidencialidad

Hace referencia a la privacidad de la información almacenada y que se procesa dentro de un sistema informático; bajo este principio, las herramientas de seguridad deben proteger el sistema de intrusos y accesos de personas o programas no autorizados.

2.1.2. Integridad

La integridad de la información, hace referencia a la validez y consistencia de la información almacenada, las herramientas de seguridad deben garantizar que los procesos de actualización estén sincronizados a fin de evitar la duplicidad de la información.

2.1.3. Disponibilidad

La disponibilidad de la información hace referencia a la continuidad de acceso a la información almacenada y procesada dentro de un sistema informático; bajo este principio, las herramientas de seguridad, deben contribuir a la permanencia de la información en un sistema.

2.2. RIESGOS DE LOS SISTEMAS INFORMÁTICOS

Según Téllez (2014, pág. 33), los riesgos informáticos son aquellos que se refieren a la incertidumbre ocasionada por la posible ejecución de una amenaza, cuya consecuencia puede

provocar daños a los servicios informáticos, instalaciones, proyectos, archivos, programas, datos y demás bienes de una organización o empresa.

2.2.1. Riesgo

El riesgo se define como la probabilidad de que se materialice o no una amenaza, debido a la presencia de vulnerabilidades existentes en un sistema informático o su entorno (Aguilera, 2010, pág. 14).

Ante un riesgo, la organización o empresa puede tomar varias alternativas:

- ✓ Asumirlo: tiene sentido asumir un riesgo cuando el perjuicio sobre un activo no tenga valor alguno
- ✓ Aplicar medidas para minimizarlo o anularlo
- ✓ Transferir el riesgo (ejemplo la contratación de un seguro)

2.2.2. Ataque

Se produce un ataque accidental o deliberadlo cuando se ha materializado una amenaza en contra de un activo.

2.2.3. Amenazas

Una amenaza según el Ministerio de Hacienda y Administraciones Públicas (2012, pág.19), se puede definir como un incidente que puede ocasionar daño a un sistema de información o a su entorno.

2.2.4. Vulnerabilidades

Una vulnerabilidad es una debilidad la cual puede ser aprovechada por una o varias amenazas para causar daños sobre un activo o sobre una organización.

2.3. SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS

Según Gómez (2007), la Seguridad Informática se puede definir como cualquier medida que sea implementada con la finalidad de impedir que se ejecute operaciones no autorizadas en un sistema o sobre una red informática y cuyos efectos puedan comprometer su integridad, confidencialidad o autenticidad, disminuir su rendimiento o permitir accesos no autorizados a un sistema, además la seguridad en los sistemas informáticos, pretende:

- ✓ Cumplir las regulaciones legales de acuerdo al tipo de empresa u organización y al país al que pertenecen.
- ✓ Registro de acceso al sistema informático
- ✓ Control de acceso a los servicios del sistema informático

2.4. LA SEGURIDAD DE LA INFORMACIÓN EN UNA ORGANIZACIÓN

.Una organización o empresa debe estar consciente de que la información es un activo importante o primordial en la continuidad del negocio, por lo cual deberá establecer medidas que apoyen a garantizar su integridad, disponibilidad y confidencialidad; sin embargo muchas de las empresas u organizaciones se centran únicamente en la aplicación de la seguridad física, dejando de lado otros aspectos de relevancia que están ligados directamente al manejo y gestión de la información, lo cual se denomina la “seguridad de la información”.

Se debe tener en cuenta que garantizar un nivel total de protección es casi imposible, pero la aplicación de políticas de seguridad de la información, tienen como propósito garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización o empresa, de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías (Hallberg y Hunstad, 2005, pág. 25).

Finalmente, la evaluación de la seguridad de la información, será importante, pues un correcto proceso de evaluación permitirá alcanzar un nivel adecuado de la seguridad de las Tecnologías de la Información.

2.5. ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

El acuerdo Ministerial 166, publicado en el Registro Oficial el 25 de septiembre de 2013, establece aplicar el Esquema Gubernamental de Seguridad de la Información (EGSI) en las entidades de la Administración Pública Central (EGSI, 2013).

Según EGSI (2013) "*El Egsi establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública. "El EGSI no reemplaza a la norma INEN ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices."*

Por otro lado, el EGSI también especifica que, de acuerdo a las necesidades de cada institución pública, dirección o departamento, se podrán especificar políticas de seguridad amplias o específicas en armonía con la Constitución, leyes y demás normativa legal propia o relacionada, así como su misión y competencias.

2.6. NORMA ISO/IEC 27000

Las organizaciones o empresas que busquen diseñar e implementar una normativa de seguridad de la información basada en estándares internacionales, deberán realizar una Política de Seguridad de la Información; este proceso podrá ser desarrollado según las normas ISO 27000 y su familia; el enfoque de buenas prácticas relacionadas a la seguridad de la información podrá sustentarse en la norma ISO/IEC 27002.

La Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC), se encargan de establecer estándares y guías de seguridad relacionadas con sistemas de gestión, la estandarización permite ser aplicadas a cualquier tipo de empresa u organización a nivel internacional, su finalidad es facilitar el comercio, intercambio de información y apoyar a la transferencia de las tecnologías a nivel mundial (Mentor, 2016).

El conjunto de normas ISO/IEC 27000 agrupa estándares de seguridad cuya finalidad es proporcionar un marco de referencia para la gestión de la seguridad, estas normas contienen las mejores prácticas recomendadas en el entorno de la Seguridad de la Información y permiten desarrollar e implementar políticas y sistemas de Gestión de Seguridad de la Información.

Tabla 1.- Familia de las Normas ISO 27000

Norma	Descripción
ISO/IEC 27000	Vocabulario estandarizado para el Sistema de Gestión de Seguridad de la Información (SGSI) y para todas las normas de la familia.
ISO/IEC 27001	Norma que puede ser certificable, a través de una auditoría, la empresa u organización debe tener implementado un SGSI.
ISO/IEC 27002	Guía de buenas prácticas a través de las cuales una organización o empresa puede mejorar la seguridad de la información.

Norma	Descripción
ISO/IEC 27003	Establece las directrices para el diseño de un SGSI durante todas sus etapas.
ISO/IEC 27004	Establece una variedad de buenas prácticas para la evaluación y medición de la gestión de la seguridad de la información.
ISO/IEC 27005	Esta norma se centra en establecer las directrices y recomendaciones para la gestión de riesgos en un SGSI.
ISO/IEC 27006	Esta norma contiene la guía y directrices para la acreditación de las organizaciones encargadas de auditar los SGSI.
ISO/IEC 27007	Establece las directrices para los organismos de certificación acreditados con la finalidad de auditar un SGSI.
ISO/IEC 27799	Establece y proporciona los controles de seguridad para la protección de la información personal en los entornos relacionados a la salud.

Fuente: Mentor, 2016

2.6.1. LA NORMA ISO 27001

La norma ISO/IEC 27001:2013 es empleada para la certificación de un Sistema de gestión de Seguridad de la información, a través del uso de esta norma una organización pude demostrar a todos sus clientes o a las organizaciones con las que guarda algún tipo de relación, la integridad en el manejo de la seguridad de su información, esta característica es un valor agregado a disponibilidad de la empresa.

La norma ISO 27001:2013 ha sido preparada con la finalidad de proporcionar los requisitos para establecer, implementar y mantener el proceso de mejora continua en un Sistema de Gestión de Seguridad de la Información. La implementación del SGSI en una empresa u organización dependerá de las necesidades, objetivos, tamaño y estructura de la organización (ISO 27001, 2013).

La norma ISO 27001:2013, especifica 10 puntos, los cuales se muestran a continuación (ISO 27001):

- ✓ **Objeto y campo de aplicación:** describe la finalidad de la norma
- ✓ **Referencias normativas**
- ✓ **Término y definiciones:** términos y definiciones de la norma ISO/IEC 27000
- ✓ **Contexto de la organización:** determinación de los aspectos externos e internos que incidan en el sistema de gestión de la seguridad de la información de la organización. En este apartado debe especificarse el alcance del SGSI.
- ✓ **Liderazgo:** hace referencia al compromiso y liderazgo que debe tener la alta dirección o gerencia de la organización en todos los procesos de la seguridad de la información, así como el compromiso de los recursos para la implementación y operatividad.
- ✓ **Planificación:** análisis, valoración y evaluación de riesgos, tratamiento de los riesgos, adicionalmente la organización debe establecer los objetivos de seguridad de la información.
- ✓ **Soporte:** trata sobre los recursos que deben asignarse para la implementación, mantenimiento y mejora continua del SGSI, competencias personales y de la importancia de la documentación de la información.
- ✓ **Operación:** el cómo se debe planificar y controlar la operación, así como la valoración de los riesgos y su tratamiento.
- ✓ **Planificar, implementar y controlar**: los procesos que satisfagan las necesidades relacionadas a la seguridad de la información, apreciación de los riesgos y el tratamiento sobre los mismos.

- ✓ **Evaluación de desempeño:** monitoreo, medición, análisis y evaluación del SGSI, adicionalmente se habla de las auditorías dentro de la organización.
- ✓ **Mejora:** hace referencia al tratamiento de las no conformidades, acciones correctivas y mejora continua.

La Norma ISO 27001:2013 en su segundo apartado contiene el anexo en el cual se establecen los objetivos de control y los controles de referencia, alineados con los enumerados en la ISO/IEC 27002:2013.

2.6.2. LA NORMA ISO 27002

La norma ISO/IEC 27002:2013, proporciona las pautas para los estándares de seguridad de la información de las empresas y organizaciones, incluye las buenas prácticas para la gestión de seguridad de la información a través de las secciones de implementación y controles de acuerdo al entorno de riesgo de seguridad de la información (International Organization for Standardization, 2017).

La Norma ISO/IEC 27002:2013, está diseñada para utilizarse por organizaciones o empresas que pretenden:

- ✓ Seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información basado en la ISO / IEC 27001
- ✓ Implementar los controles de seguridad de la información
- ✓ Desarrollar sus propias políticas de seguridad de la información.

La norma ISO 27002:2013 está dividida en 14 capítulos dentro de los cuales se especifican las áreas a tener en cuenta con la finalidad de garantizar la seguridad de la información, dentro de una organización o empresa (ISO Tools Excellence, 2016).

En la norma existen un total de 114 controles, a continuación se resumen los 14 capítulos:

1. **Políticas de Seguridad de la Información**

Capítulo dedicado a la importancia o el rol primordial que juega la dirección o alta gerencia en la disposición de una adecuada política de seguridad; esto implica: su aprobación, revisión, actualización y socialización al personal de la organización.

2. **Organización de la Seguridad de la Información**

A través de los roles, tareas, seguridad; los controles abarcados en este capítulo, buscan estructurar un marco referencial de seguridad.

Debido a que en la actualidad en muchas empresas se aplica el teletrabajo (trabajo a distancia), se debe tener en cuenta cada aspecto de este tipo de trabajo, para que en ningún momento la seguridad de la información se vea comprometida.

3. **Seguridad relativa a los recursos humanos**

Hace referencia a la importancia de la socialización, concientización y formación del personal en los temas de la utilización de la información y la importancia de ésta en el desarrollo de sus actividades. El recurso humano es directamente responsable de mantener la seguridad dentro de su organización, de ahí la importancia de promover, mantener y mejorar el nivel de seguridad, adecuándolo a las necesidades de la organización.

4. Gestión de activos

En la actualidad la información es considerada como uno de los activos más importantes en una organización, este capítulo centra su atención en la manera de establecer las medidas adecuadas que garanticen la confidencialidad, integridad y disponibilidad de la información.

5. Control de acceso

Centra su análisis en la gestión del acceso a la información. De acuerdo a los roles que desempeña cada empleado de la organización, se deberán establecer y gestionar los privilegios de acceso, en este apartado se incluyen los controles relacionados al acceso de la información.

6. Criptografía

A través de las técnicas criptográficas, es posible el tratamiento de la información considerada como sensible o crítica; este apartado hace referencia a la importancia de garantizar la seguridad de la información mediante la criptografía.

7. Seguridad física y del entorno

Las áreas de procesamiento y almacenamiento de la información considerada como sensible o crítica deben ser seguras y deben estar protegidas por perímetros de seguridad, este apartado hace referencia a la protección física de la información, evitando el acceso no autorizado a las instalaciones donde se almacene la misma.

8. Seguridad de las operaciones

Considera aspectos relacionados a los componentes técnicos como la protección contra software malicioso, copias de seguridad o gestión de vulnerabilidades.

9. Seguridad de las comunicaciones

Se enfoca en garantizar la seguridad de la información, a través de la protección adecuada de los medios de transmisión de los datos.

10. Adquisiciones, desarrollo y mantenimiento de los sistemas de información

La seguridad de la información abarca a toda la organización y debe estar presente como elemento transversal en el ciclo de vida del SGSI.

11. Relación con los proveedores

Los acuerdos, compromisos, contratos y demás relaciones establecidas con terceros, deben contener las medidas necesarias que garanticen la seguridad de la información, esto es su confidencialidad, integridad y disponibilidad.

12. Gestión de incidentes de seguridad de la información

Hace referencia a los controles de seguridad encaminados a la atención rápida y oportuna frente a los incidentes de seguridad de la información, esto es: previo, durante y después de un incidente.

13. Aspectos de seguridad de la información para la gestión de la continuidad del negocio

Sufrir la pérdida de información puede traer consecuencias graves a una organización o empresa, aquí tiene suma importancia la capacidad que tenga la organización de seguir con sus operaciones después de haber sufrido cualquier tipo de incidente.

14. Cumplimiento

Uno de los aspectos más importantes al hablar de seguridad de la información son las normativas, políticas y legislaciones con las cuales conviven las organizaciones; la socialización y cumplimiento de las normas contribuyen a mejorar la gestión de la seguridad de la información.

2.7. DEFINICIÓN E IMPLANTACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Según Gómez (2011), al referirse a los conceptos de seguridad de la información, se puede manejar la siguiente jerarquía:

Figura 1.-Jerarquía en los conceptos de Seguridad de la Información
Fuente: (Gómez, 2011)

CIA: corresponde a los objetivos fundamentales de la Gestión de la Seguridad de la Información (Confidencialidad, integridad y disponibilidad de la Información).

Políticas de seguridad: Una Política de seguridad se define como una "declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran*"* (Gómez, 2011).

Plan de seguridad: es el conjunto de decisiones para realizar acciones futuras y los medios que se deben utilizar para ejecutar las mismas.

Procedimiento de seguridad: es la definición y detalle de los pasos que deben seguirse para ejecutar tareas determinadas; un procedimiento de seguridad permite aplicar las políticas de seguridad en una empresa u organización.

Finalmente los procedimientos de seguridad pueden dividirse en tareas y operaciones específicas y estas pueden generar registros y evidencias.

2.7.1. Definir la política

Al momento de plantear una política de seguridad en una organización, pueden surgir varias interrogantes como: ¿Quiénes son los responsable de desarrollar la política?, ¿Qué debe abarcar la política?, ¿Qué debe contener la política?, ¿Cómo hacer cumplir la política?, para ello se presenta las siguientes etapas (Mendez et al., 2003, pág. 187):

2.7.1.1.Planeación de las políticas:

Contar con el apoyo de la alta dirección, conocer la postura de la organización, detectar la problemática a través de un análisis de riesgos y definir que se va a proteger.

2.7.1.2.Iniciar su desarrollo

Designar a una persona como responsable del proceso de la política y de dar el seguimiento a la misma.

2.7.1.3.Redacción de la política

Hacer partícipes a los conocedores de los procesos, de tal forma que aporten información sobre los aspectos críticos de los sistemas tecnológicos y sobre la organización; cómo características que debe tener la política, se contemplan los siguientes aspectos:

- ✓ Enfocar la política hacia la problemática de la organización o empresa
- ✓ El documento debe tener una estructura bien definido
- ✓ Los enunciados deben ser claros y precisos
- ✓ Exponer de manera explícita el ámbito de la aplicación
- ✓ Establecer obligaciones y derechos para los usuarios y administradores
- ✓ Definir claramente las sanciones a quienes violaran las políticas establecidas
- ✓ El documento debe tener vigencia y flexibilidad para realizar actualizaciones

2.7.1.4.Aprobación y difusión

Posteriormente la política debe ser aprobada por el cuerpo directivo y finalmente debe ser socializada todos los empleados o trabajadores.

2.8. METODOLOGÍA PARA EL ANÁLISIS DE RIESGOS (METODOLOGÍA MAGERIT)

Magerit es una metodología que implementa el proceso de Gestión de Riesgos en un marco de trabajo enfocado a los órganos de gobierno con el propósito que éstos tomen las decisiones teniendo presente los riesgos derivados del uso de las tecnologías de la información y sus entornos (Ministerio de Hacienda y Administraciones Públicas. 2012).

A través de la metodología MAGERIT se realiza un análisis ordenado y sistemático de los activos de la organización, las amenazas sobre los activos, estimación del impacto, estimación del riesgo; este análisis puede ser resumido en la matriz de riesgos. Finalmente a través de la norme NTE INEC ISO/IEC 27002:2013 se podrá seleccionar los controles necesarios sobre los riesgos encontrados. A continuación se describen el proceso de análisis de riegos a través de la metodología Magerit:

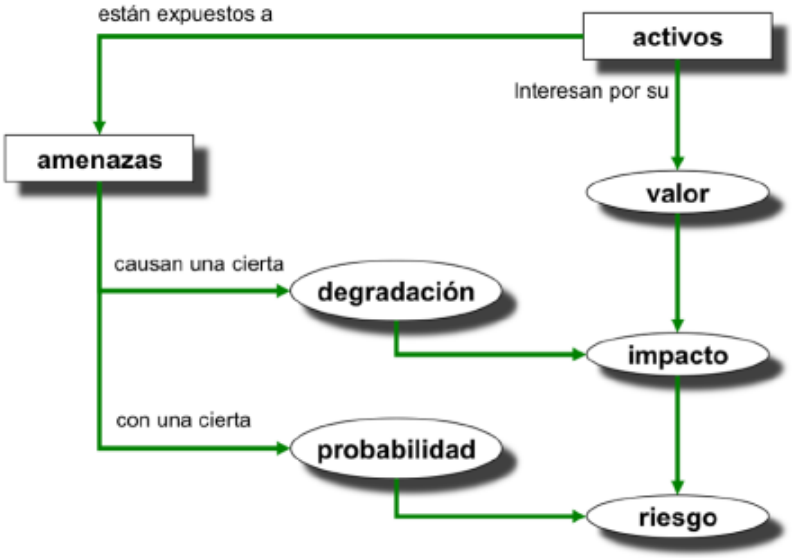

Figura 2.- Análisis del riesgo a través de Magerit
Fuente: *(*Ministerio de Hacienda y Administraciones Públicas, 2012, pág.22)

2.8.1. Determinar los activos de la organización

El primer paso será determinar los activos de la organización, para este análisis se establece un catálogo de activos relevantes, se deberá clasificar los activos dentro de una de las siguientes categorías:

- ✓ **Datos:** los que materializan la información

- ✓ **Servicios:** necesarios para organizar el sistema
- ✓ **Software – aplicaciones informáticas:** lo que permite manejar y administrar los datos
- ✓ **Hardware- equipos informáticos:** lo que permite alojar los datos, aplicaciones e información
- ✓ **Soportes de información:** dispositivos de almacenamiento
- ✓ **Equipamiento auxiliar:** que complementan el material informático
- ✓ **Redes de comunicaciones:** los que permiten intercambiar datos
- ✓ **Las instalaciones:** donde se hospeda los equipos y el personal humano
- ✓ **Las personas:** recurso humano

Posteriormente se realiza una valoración de activos, basado en la afectación que tendría el activo en relación a su disponibilidad, confidencialidad e integridad.

A continuación, se muestra la tabla para la valoración de los activos; se deberá establecer una valoración individual para la disponibilidad, integridad y confidencialidad, el promedio de estos tres criterios de seguridad de la información, establecerá la criticidad del activo:

Tabla 2.- Valoración de los activos

AFECTACIÓN	DESCRIPCIÓN	VALORACIÓN
Extremo	Extremadamente grave	5
Muy alto	Muy grave	4
Alto	Grave	3
Medio	Importante	2
Bajo	Menor	1
Despreciable	Irrelevante	0

Fuente: (Ministerio de Hacienda y Administraciones Públicas. 2012, pág. 19)

2.8.2. Determinar las amenazas a las cuales están expuestas los activos

Según el Ministerio de Hacienda y Administraciones Públicas (2012, pág.27), existe una relación de amenazas típicas que pueden causar daños a los sistemas de información y a sus entornos. La Metodología Magerit, establece un listado de amenazas de acuerdo a su origen las cuales se presentan a continuación:

- ✓ **De origen natural:** corresponden a las amenazas originadas en la naturaleza, las mismas que no son predecibles y no pueden ser controladas como los terremotos, erupciones volcánicas, inundaciones, tsunamis, entre otras; ante uno de estos eventos un sistema de información o su entorno es una víctima pasiva, estas amenazas no pueden evitarse, pero se deben tener en cuenta.
- ✓ **Del entorno:** conocidos también como desastres industriales por ejemplo la contaminación o los fallos eléctricos; los sistemas de información o sus entornos también son víctimas pasivas ante estas amenazas.
- ✓ **Defectos de las aplicaciones:** problemas relacionados al equipamiento de los sistemas informáticos (en su diseño, implementación u operación), se denominan también vulnerabilidades técnicas.
- ✓ **Causadas por las personas de forma accidental:** relacionados a los errores u omisiones (acciones no intencionadas), ocasionadas por personas que tienen acceso a las plataformas tecnológicas o al entorno de la organización.
- ✓ **Causadas por las personas de forma deliberada:** ocasionadas por personas que tienen acceso a las plataformas tecnológicas o al entorno de la organización, las acciones son ejecutadas de forma mal intencionada e indebidamente con la finalidad de obtener beneficio o causar un daño a la organización o a una persona en específico.

Las amenazas deberán estar asociadas a la posible afectación que puedan ocasionar sobre la disponibilidad, integridad y confidencialidad de la información de un activo. En el capítulo III desde la Tabla 6 hasta la Tabla 12, se muestra las amenazas determinadas en relación a los activos del Sistema de Botones de Seguridad.

2.8.3. Estimar el impacto

Se denomina impacto a la medida del daño sobre un activo o sobre la organización, ocasionado por la materialización de una amenaza (Ministerio de Hacienda y Administraciones Públicas, 2012, pág.28).

La estimación del impacto será calculada con los valores determinados de la valoración de activos y la degradación de los mismos.

Degradación: según el Ministerio de Hacienda y Administraciones Públicas (2012. pág. 28), cuando una activo es víctima de una amenaza, este pierde parte de su valor o sufre un "porcentaje de degradación del activo", esta degradación ´puede ser representada por un valor contenido entre 0% y 100%.

El resultado del impacto estará definido en los valores cualitativos: **MB:** muy bajo, **B:** bajo, **M:** medio, **A:** alto, **MA:** muy alto, de acuerdo a la siguiente figura:

IMPACTO		DEGRADACIÓN		
		B	M	A
VALOR ACTIVO	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Figura 3.- Valoración del impacto
Fuente: (Ministerio de Hacienda y Administraciones Públicas 2012, pág. 6)

2.8.4. Estimar el riesgo

El siguiente paso de acuerdo a la Metodología de Margerit es estimar el riesgo, el mismo que puede ser modelado por la combinación entre el impacto y la frecuencia de ocurrencia (Ministerio de Hacienda y Administraciones Públicas, 2012, pág. 22).

Probabilidad

Según Fernández (2018), la probabilidad es la posibilidad de que un riesgo analizado ocurra o se materialice, en este sentido se está hablando de una probabilidad teórica debido a que una cuantificación exacta no es posible, pues un riesgo cero no existe.

La probabilidad puede ser cuantificada de acuerdo a la siguiente figura:

PROBABILIDAD	DESCRIPCIÓN	FRECUENCIA
MA: Prácticamente seguro	Muy frecuente	Diario – semanal
A: Probable	Frecuente	Mensual
M: Posible	Normal	Una vez al año
B: Poco probable	Poco frecuente	Cada varios años
MB: Muy raro	Muy poco frecuente	Siglos

Figura 4.- Estimación de la probabilidad
Fuente: (Ministerio de Hacienda y Administraciones Públicas 2012, pág. 18)

El impacto puede ser evaluado en base a la siguiente figura:

RIESGO		PROBABILIDAD				
		MB	B	M	A	MA
IMPACTO	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	

Figura 5.- Valoración del impacto
Fuente: (Ministerio de Hacienda y Administraciones Públicas 2012, pág. 7)

2.8.5. Determinar las salvaguardas

Las salvaguardas conocidas también como contramedidas, serán los mecanismos y procedimientos que permiten reducir el riesgo

Para la selección de salvaguardas se debe considerar los siguientes aspectos:

- ✓ Tipos de activos a proteger
- ✓ Dimensión de seguridad que requieren protección
- ✓ Amenazas ante las cuales se debe proteger los activos
- ✓ Considerar salvaguardas alternativas

La selección de los controles dependerá de las necesidades y prioridades de la organización, basados en el criterio de aceptación del riesgo, para este efecto se seleccionará los controles descritos en la Norma INEN ISO/IEC 27002:2013.

CAPÍTULO III

ANÁLISIS Y SITUACIÓN ACTUAL

3.1.SITUACIÓN ACTUAL

3.1.1. ANTECEDENTES

Las Unidades de Policía Comunitaria (UPC) juegan un papel fundamental en el nuevo modelo de gestión de la Policía Nacional, donde el acercamiento a la ciudadanía es la base para los programas de prevención de delitos, así como el centro de integración de los barrios y comunidades en torno a la seguridad, esto sumado a la constante innovación de la tecnología y su aplicación en los procesos cotidianos han sido un pilar fundamental en el desarrollo de sistemas integrales de seguridad, en este sentido nace el Sistema de Botones de Seguridad como un servicio de atención a la ciudadanía.

El sistema de botones de seguridad, tiene como finalidad brindar un servicio de atención oportuno a la ciudadanía a través de la generación de alertas; en caso de presentarse algún tipo de emergencia un ciudadano a través de su teléfono celular o convencional, puede solicitar la presencia Policial de manera directa a la UPC de su sector.

El personal policial de cada una de las UPC a nivel nacional, realiza el monitoreo del sistema de acuerdo a su zona de responsabilidad, la administración de la plataforma a nivel nacional, está a cargo de la Coordinación General de las Tecnologías de la Información y

Comunicación del Ministerio del Interior, la infraestructura de la plataforma tecnológica se encuentra alojada en una empresa proveedora de servicios tecnológicos.

3.1.2. EL SISTEMA DE BOTONES DE SEGURIDAD

El Sistema de Botones de Seguridad es un Sistema Integral de Seguridad, se encuentra compuesto por una plataforma tecnológica, una unidad técnica – administrativa, una unidad de coordinación y la unidad de operación; enmarcado bajo los lineamientos de la Coordinación General de Tecnologías de la Información del Ministerio del Interior en coordinación con la Policía Nacional.

3.1.2.1. Plataforma Tecnológica

Se refiere a la infraestructura, componentes, servicios y demás solucciones tecnológicas que forman parte del Sistema de Botones de Seguridad, administrado por la Unidad Técnica – Administrativa.

3.1.2.2. Unidad Técnica Administrativa

Unidad encargada y responsable de la gestión administrativa del Sistema de seguridad Integral, administra la plataforma tecnológica, coordina y da atención a las solicitudes de la Policía Nacional en el ámbito de su competencia, capacita y socializa el sistema y brida la asistencia y/o soporte técnico de la plataforma tecnológica.

3.1.2.3. Unidad de Coordinación

Unidad integrada por personal de la Dirección Nacional de Policía Comunitaria, establece los lineamientos y genera los requerimientos y funcionalidades en los aplicativos y sistema web, emite las disposicones y demás directrices al personal de las Unidades de Policía Comunitaria.

3.1.2.4. Unidad Operativa

Corresponde a la participación de las Unidades de Policía Comunitaria (UPC) como centro de monitoreo y atención a las emergencias a nivel de su zona de rsponsabilidad (Circuito o Sub Circuito). Mediante un sistema web accesible con un perfil de usuario específico, se realiza el monitoreo de los botones de seguridad de los ciudadanos registrados en la zona de responsabilidad de la UPC.

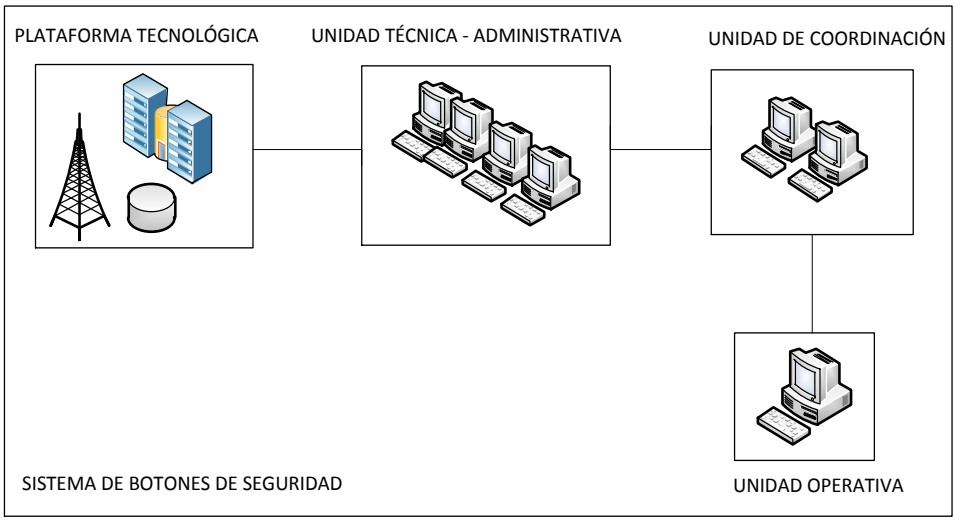

Figura 6.- Estructura organizativa-Sistema de Botones de Seguridad
Fuente: (DSTU/MDI, 2018)

3.1.3. SERVICIOS QUE INTEGRAN LA PLATAFORMA TECNOLÓGICA DE BOTONES DE SEGURIDAD

3.1.3.1. SISTEMA WEB

Servicio que alberga el sistema web y aplicativos para la administración del MDI, y la gestión del sistema por parte de la Policía Nacional, de acuerdo a los siguientes parámetros generales:

- Acceso al sitio web mediante conexión segura (https).
- Administración y creación de usuarios en diferentes perfiles y niveles según la distribución SENPLADES.
- Registro y configuración de datos de ciudadanos y policías.
- Monitoreo, seguimiento y cierre de alarmas.
- Generación de reportes de registros de ciudadanos, policías y alarmas.
- Clasificación de alarmas por tipos de incidentes.
- Reportes de acuerdo a la distribución SENPLADES y División Política Administrativa (DPA), por fechas día/mes/año, rangos definidos de acuerdo a cada perfil de usuario.
- Presentación de los mapas geográficos a nivel nacional con actualización periódica.
- Manejo de reportes con todos los datos históricos.
- Validación de datos mediante conectividad con la Base de Datos del Registro Civil.

3.1.3.2. IVR (INTERACTIVE VOICE RESPONSE)

IVR (Interactive Voice Response) o respuesta de voz interactiva, 7 canales simultáneos para llamadas entrantes, respuesta automática a llamadas del ciudadano para alertas de seguridad a través de los números asignados que enrutan la emergencia a la UPC correspondiente.

3.1.3.3. INTEGRADOR DE SERVICIOS SMS

Servicio para la notificación de emergencias a través SMS

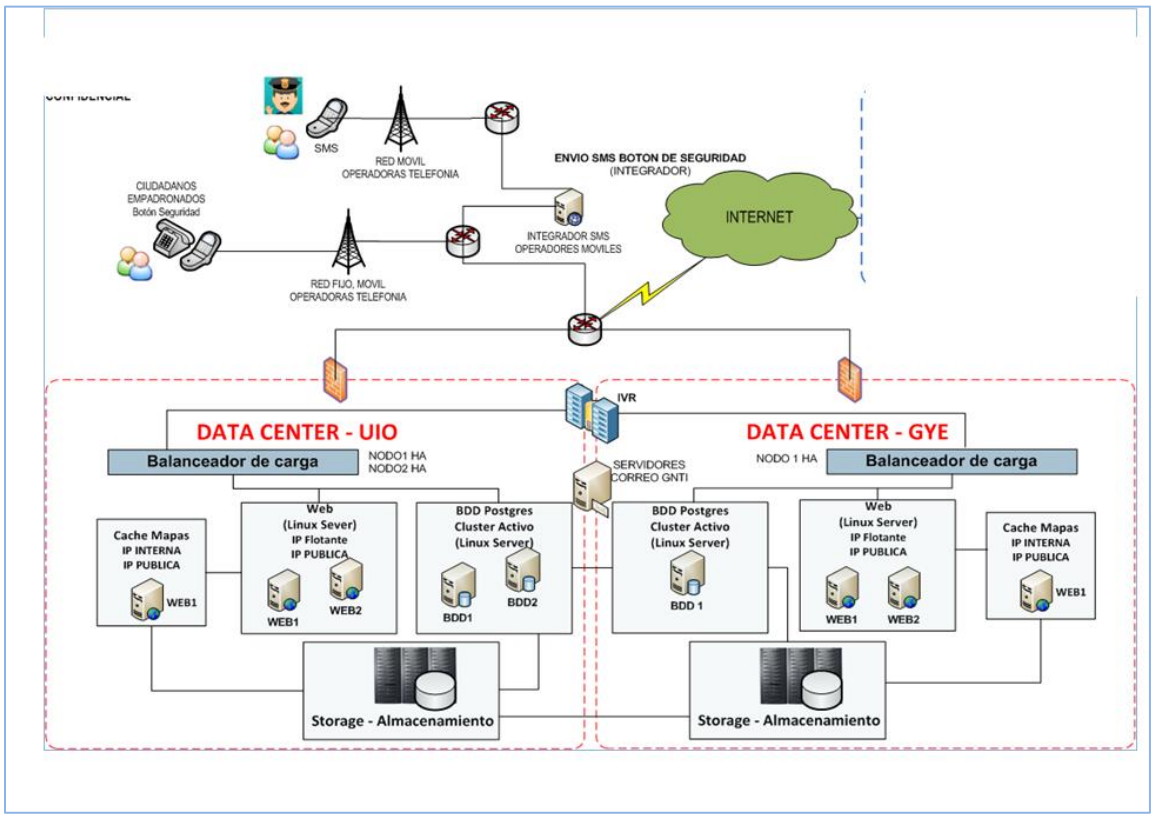

Figura 7.- Esquema de la Plataforma Tecnológica
Fuente: (DSTU/MDI, 2018)

3.1.4. ESQUEMA DE ATENCIÓN A LAS EMERGENCIAS A TRAVÉS DEL SISTEMA DE BOTONES DE SEGURIDAD

A continuación se muestra y describe el esquema de atención a emergencias a través del Sistema de Botones de Seguridad:

1. El ciudadano registra en un formulario los datos de su domicilio o local comercial en la UPC más cercana, una vez que sus datos son ingresados al sistema, el ciudadano recibe un SMS de confirmación de registro, adicionalmente el personal policial le configura al ciudadano una tecla de marcación rápida o le informa al ciudadano la manera en la que puede generar una alerta.
2. El ciudadano registra en un formulario los datos de su domicilio o local comercial en la UPC más cercana, una vez que sus datos son ingresados al sistema, el ciudadano recibe un SMS de confirmación de registro, adicionalmente el personal policial le configura al ciudadano una tecla de marcación rápida o le informa al ciudadano la manera en la que puede generar una alerta.

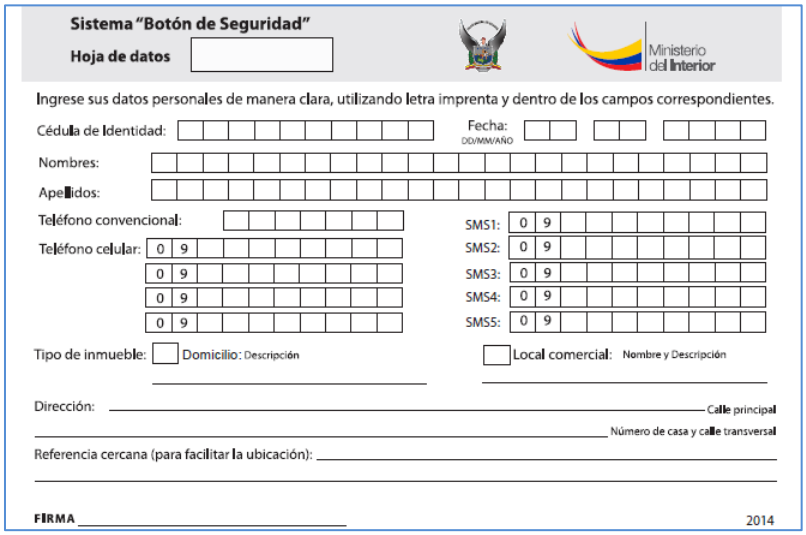

Figura 8.- Formulario de registro para activación del servicio
Fuente: (DSTU/MDI, 2018)

3. El ciudadano genera la alarma mediante la marcación directa de la tecla 5 desde su teléfono celular o mediante el número indicado por el personal policial.
4. La alarma generada envía una trama al integrador SMS y al Sistema Web de la Plataforma.
5. En la computadora de la UPC en el sistema web de Botones de Seguridad, se recibe una notifiación de la emergencia, la plataforma también notifica mediante mensajes de texto que son enviados a los teléfonos de los policías que se encuentran de servicio en la UPC para que se pueda dar atención a la emergencia.
6. Una vez que ha sido atendida la emergencia, el personal policial de la UPC registra los datos en un formulario en línea, el ciudadano también recibe un SMS informándole datos referente a la emergencia atendida.

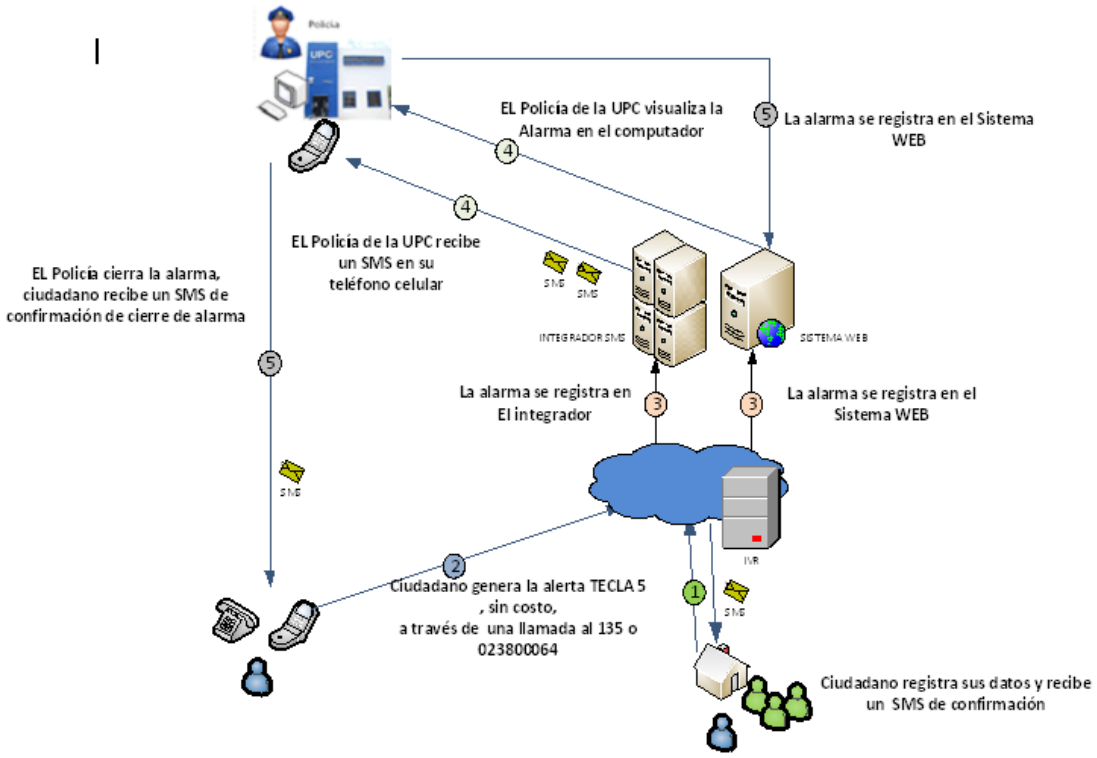

Figura 9.- Esquema de atención a las emergencias
Fuente: (DSTU/MDI, 2018)

3.1.5. GESTIÓN DE LA INFORMACIÓN

3.1.5.1. Seguridad Física

La plataforma tecnológica del Sistema de Seguridad se encuentra físicamente alojada en el Data Center de una empresa proveedora de servicios tecnológicos, la misma que tiene redundancia de servicios en otro Data Center en una ciudad diferente del país.

En el contrato suscrito con la empresa proveedora del servicio, se contempla como parte de un claúsula que: *"los recursos tecnológicos asignados a la Plataforma de Botones de Seguridada, deberán estar alojados en el Data Center con características de seguridad para información crítica y sensible "*

Por otra los formularios de inscripciones de ciudadanos, reposan en la oficinas del archivo central del MDI, si bien se encuentran bajo custodia, no se ha establecido un proceso debido para el archivo de las mismas.

De igual manera carpetas que contienen información como manuales de usuarios, contratos, acuerdos de confidencialidad, manuales de procesos, asignaciones de cuentas de usuarios, reposa en las oficinas de la Unidad Técnica Administrativa de Botones de Seguridad, esta documentación se encuentra en archivadores pero no se encuentran debidamente cerrados con llaves.

La Unidad de Coordinación y Unidad de Operación no tienen acceso físico a la información del Sistema de Seguridad, el acceso se lo realiza a través de los aplicativos mediante un sistemas web.

3.1.5.2. Tipo de información

3.1.5.2.1. Registros Ciudadanos

Módulo de almacenamiento y registro de datos de ciudadanos, los registros contienen información de tipo personal, así como la información asociada a los domicilios o locales comerciales de los ciudadanos registrados, además se incluye la georeferenciación de los registros.

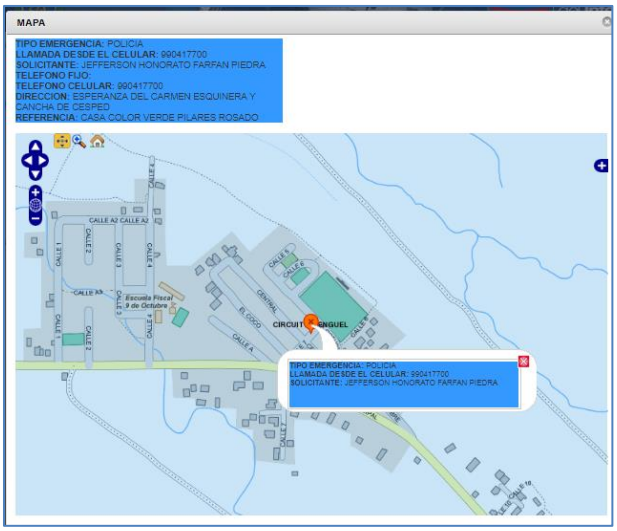

Figura 10.- Registros ciudadanos geo referenciados
Fuente: (DSTU/MDI, 2018)

3.1.5.2.2. Registro - Personal Policial

Módulo correspondiente a los datos o registros del personal policial que labora en la UPC, la importancia de este módulo a más de los datos del personal policial, radica en que en este modulo se registran los celulares del personal policial al cual se notifican las alarmas.

3.1.5.2.3. Monitoreo de Emergencias

Módulo de monitoreo de las emergencias en tiempo real.

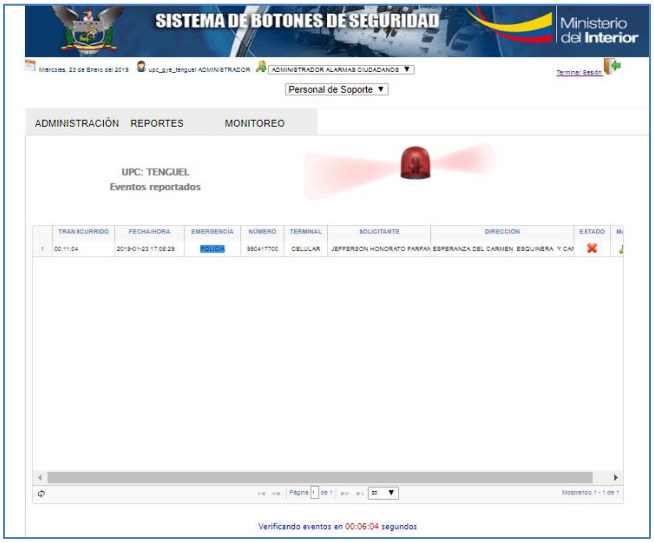

Figura 11.- Monitoreo de emergencias
Fuente: (DSTU/MDI, 2018)

3.1.5.2.4. Sistema Integrador de SMS

Sistema web de acceso al detalle de SMS enviados, tiempos y detalle del texto enviado.

3.1.5.2.5. Sistema de reportería.

Módulo de reportería, estadísticas, datos, incidentes y demás variables relacionados a la atención a emergencias a través del Sistema de Botones de Seguridad.

3.1.5.3. Acceso a la información

En primera instancia y como medida de protección y confidencialidad de la información física alamcenada en el Data Center, se ha establecido un acuerdo de Confidencialidad de la información entre el MDI y la empresa proveedora de servicios tecnológicos, en la cual se expresa:

- "Tratar los datos y la información del Ministerio del Interior como datos e información crítica y confidencial" (DSTU/MDI, 2018b).

- "Bajo ninguna circunstancia y por ningún motivo el oferente del servicio podrá entregar los datos y la información del Ministerio del Interior a terceros, salvo autorización por escrito del Ministerio del Interior" (DSTU/MDI, 2018b).

Sin embargo hay que considerar que el acceso a la información, principalmente al Sistema Web, se la realiza de manera remota de acuerdo a los perfiles y cuentas asignadas; en la siguiente tabla se muestra el inventario de usuarios asignados:

Tabla 3.- Perfiles y usuarios del sistema Web de Botones de Seguridad

PERFIL DE USUARIO	DESCRIPCIÓN	USUARIOS ASIGNADOS
OPERADOR	Usuario para cada UPC: Gestión, operación y atención a incidencias dentro de su zona de responsabilidad Acceso únicamente a la información de su zona de responsabilididad (circuito o subcircuito)	1259
DISTRITO	Asignado a los Jefes de Distrito o sus delegados, permite realizar la supervisión y generación de reportes Acceso únicamente a la información de su zona de responsabilididad (Distrito, circuitos y subcircuitos)	140
INSPECTOR	Perfil de usuario para la supervisión a nivel nacional Acceso a la información a nivel nacional	2
SUPERVISORES	Perfil de usuario para administración y supervisión a nivel nacional Acceso a la información a nivel nacional	10
ADMINISTRADOR	Administración total del MDI sobre el sistema Web	--

Fuente: (DSTU/MDI, 2018)

De la tabla anterior, se tiene como un punto relevante a considerar, que debido al número de cuentas y usurios asignados es necesario establecer controles que se enfoquen en la seguridad de las contraseñas y gestión de accesos a diferentes perfiles de usuarios.

3.1.5.4. Registro de cambios en las aplicaciones y sistema web de la plataforma tecnológica

Las solicitudes de cambios, modificaciones o funcionalidades principalmete en el sistema y aplicativo web de botones de seguridad, es solicitado por la Dirección Nacional de Policía Comunitaria a través de un documento formal dirigido a la Coordinación de Tecnologías de la Información del Ministerio del Interior.

Mediante un análisis, se determina la factibilidad técnica y a través de un Documento de Especificaciones Funcionalidades DEF se realiza la implementación o cambios en las funcionalidades a través de la empresa proveedora del servicio; si bien existe un proceso o lineamiento estructurado, el mismo no se encuentra documentado.

3.1.5.5. Cambios en el hardware de la plataforma tecnológica

Cualquier cambio de hardware en la plataforma tecnológica, implica poner en conocimiento de los administradores de la plataforma de Botones de Seguridad, las tareas y actividades específicas a ejecutarse, además de realizarse una ATP (Acta Técnica de Pruebas) como validación de los cambios realizados.

3.1.6. DE LA SEGURIDAD DE LA INFORMACIÓN

De acuerdo las entrevistas realizadas al personal que trabaja en esta unidad, se determina los siguientes aspectos:

- ✓ Si bien existe el EGSI a nivel de toda la institución pública, este no ha sido debidamente socializado.
- ✓ El EGSI establece aspectos generales sobre la gestión de la información, no es específico en ciertos aspectos o procedimientos.
- ✓ Fácil acceso físico a la documentación como contratos, manuales de usuario, manuales de procedimientos, diagramas y demás documentación archivada en carpetas.
- ✓ No existe un proceso adecuado para el almacenamiento o archivo de los formularios de las inscripciones de los ciudadanos.
- ✓ No existe una metodología adecuada para respaldar la información.
- ✓ No existe un procedimiento debidamente establecido y documentado para la entrega de la información considerada como confidencial.
- ✓ Se requiere mejorar los procesos en la asignación y entrega de cuentas de usuario.
- ✓ Se requiere actualizar los procedimientos relacionados a la gestión de incidentes en caso de la indisponibilidad de servicios del Sistema de Botones de Seguridad.
- ✓ No siempre se mantienen las computadoras bloqueadas o suspendidas cuando un funcionario no está presente.

3.2. ANÁLISIS DE RIESGOS

3.2.1. APLICACIÓN DE LA METODOLOGÍA MAGERIT

Para el análisis y valoración de riesgos se ha aplicado la metodología MAGERIT, para este efecto se seguirán los pasos descritos en el Capítulo II.

3.2.1.1. Determinar los activos relevantes de la organización

Según la norma ISO (27001), los activos se definen como los recursos del Sistema de Seguridad de la Información necesarios para que una organización o empresa logre cumplir los objetivos propuestos por la alta dirección; en la siguiente tabla se muestran los activos identificados y categorizados de acuerdo a la metodología MAGERIT:

Datos o Información

- ✓ Base de datos de registros: ciudadanos, policías, alarmas o eventos atendidos y reportes de SMS

Servicios

Servicios alojados en el Centro de Datos de la Empresa proveedora de servicios

- ✓ Sistema web
- ✓ IVR
- ✓ Servicio Integrador SMS
- ✓ Sistema de Monitoreo de Servicios

Aplicaciones Informáticas – Software

- ✓ Sistema de Soporte y asistencia técnica

Equipos informáticos – Hardware

- ✓ Computadoras

Soporte de Información

- ✓ Carpetas y demás documentación física

Redes de comunicaciones

- ✓ Red de comunicaciones del MDI

Instalaciones

- ✓ Oficina Técnica Administrativa
- ✓ Oficina Dirección Nacional de Policía Comunitaria
- ✓ Oficina de la UPC (Unidad de Policía Comunitaria)

Las personas

- ✓ Director / Coordinador
- ✓ Personal Técnico – administrativo
- ✓ Personal de las UPC

Este primer análisis ha permitido identificar los activos que forman parte del Sistema de Botones de Seguridad del Ministerio del Interior.

3.2.1.1.1. Realizar la valoración de los activos

La valoración de los activos se lo realiza a través de un análisis cualitativo, es decir dicha valoración queda a discreción del usuario o conocedor del proceso; para facilitar esta evaluación, se plantea tres interrogantes relacionadas a las propiedades de la información (Disponibilidad, Integridad y Confidencialidad) y finalmente se establece una escala de correspondencia entre los criterios de afectaciones y un valor numérico.

Las interrogantes a contestar son las siguientes:

- ✓ **Disponibilidad:** ¿Que afectación tendría al Sistema Integral de Seguridad (Botones de Seguridad) el no poder utilizar el siguiente activo?
- ✓ **Integridad:** ¿Que afectación tendría al Sistema Integral de Seguridad (Botones de Seguridad) que el siguiente activo haya sido alterado o modificado?

- ✓ **Confidencialidad:** ¿Que afectación tendría al Sistema Integral de Seguridad (Botones de Seguridad) que una persona que no esté autorizada, conozca o tenga acceso al siguiente activo?

La valoración del activo depende de la afectación sobre el mismo, para esta valoración se ha utilizado la Tabla 2.- Valoración de activos, descrita en el Capítulo II.

La valoración establecida, proporciona una perspectiva de los activos que de acuerdo a su importancia, requieren una priorización o mayor grado de protección.

Tabla 4.- Valoración de activos de acuerdo a su criticidad

CATEGORIZACIÓN	ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	PROM	VALORACIÓN
Datos - Información	Base de datos de registros: ciudadanos, policías, alarmas o eventos atendidos y reportes de SMS	5	5	5	5	MUY ALTO
Servicios	Sistema web	4	5	5	4,7	MUY ALTO
	IVR	5	5	5	5	MUY ALTO
	Servicio Integrador SMS	5	5	5	5	MUY ALTO
	Sistema de Monitoreo de Servicios	5	5	4	4,7	MUY ALTO
Aplicaciones Informáticas – Software	Sistema de Soporte y asistencia técnica	2	4	4	3,3	MEDIO
Equipos informáticos – Hardware	Computadoras	4	4	4	4	ALTO

CATEGORIZACIÓN	ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	PROM	VALORACIÓN
Redes de comunicaciones	Red de comunicaciones del MDI	5	5	5	5	MUY ALTO
Instalaciones	Oficina Técnica Administrativa Oficina Dirección	3	2	2	2,3	MEDIO
	Nacional de Policía Comunitaria	3	2	2	2,3	MEDIO
	Oficina de la UPC (Unidad de Policía Comunitaria)	4	2	3	3	MEDIO
Las personas	Director / Coordinador	5	2	5	4	ALTO
	Personal Técnico – administrativo	5	4	5	4,7	MUY ALTO
	Personal de las UPC	5	2	5	4	ALTO

Fuente: Elaborado por el autor de la Investigación

A través de la valoración de activos, se determina que la información almacenada en la base de datos, los servicios, las redes de comunicaciones y el personal técnico administrativo constituyen los activos más críticos y sensibles del Sistema de Botones de Seguridad.

Se establece una valoración final de los activos, el cual será un promedio de la afectación a la disponibilidad, integridad y confidencialidad; esta valoración será considerada de acuerdo a la siguiente tabla:

Tabla 5.- Valoración de activos - Rangos

VALORACIÓN DEL ACTIVO	DESCRIPCIÓN DE LA AFECTACIÓN AL ACTIVO	Rangos
Muy Alto	Muy grave	4,5 < x < 5
Alto	Grave	3,5 < x <= 4,5
Medio	Medianamente grave	2 < x <= 3,5
Bajo	Importante	0,5 < x <= 2
Medio Bajo	Menor	0 < x <= 0,5
Despreciable	Irrelevante	0

Fuente: Elaborado por el autor de la investigación

3.2.1.2. Determinar las amenazas a las que están expuestas los activos

De la Tabla 4, correspondiente a los activos del sistema de Botones de Seguridad, se identifica las amenazas, de acuerdo al "Catálogo de Elementos", presentado en la Metodología de Análisis y Riegos de Magerit.

De acuerdo a la descripción realizada en el capítulo II, las amenazas tienen un origen o causa en los siguientes aspectos:

- ✓ De origen natural
- ✓ Del entorno
- ✓ Defectos de las aplicaciones
- ✓ Causadas por las personas de forma accidental
- ✓ Causadas por las personas de forma deliberada

A continuación se asocia cada uno de los activos del Sistema de Botones de Seguridad, con las posibles amenazas a las cuales están expuestos. Las amenazas corresponden a las

descritas en el Catálogo de Elementos de la Metodología Magerit y su respectiva afectación en los grados de integridad, disponibilidad y confidencialidad.

3.2.1.2.1. Datos o Información

Tabla 6.- Amenazas respecto a los datos o información

Activo: Base de datos de registros: ciudadanos, policías, alarmas o eventos atendidos y reportes de SMS			
N°	**Código**	**Amenaza**	**Dimensión de la afectación** **Integridad [I]** **Disponibilidad [D]** **Confidencialidad [C]**
1	[E.1]	Errores de usuarios	[I], [D], [C]
2	[E.2]	Errores del administrador	[I], [D], [C]
3	[E.15]	Alteración accidental de la información	[I]
4	[E.18]	Destrucción de la información	[D]
5	[E.19]	Fugas de información	[C]
6	[A.6]	Abusos de privilegio de acceso	[I], [D], [C]
7	[A.11]	Acceso no autorizado	[I], [C]
8	[A.15]	Modificación deliberada de la información	[I]
9	[A.18]	Destrucción de la información	[D]
10	[A.19]	Divulgación de la información	[C]

Fuente: elaborado por el autor de la Investigación

3.2.1.2.2. Servicios

Tabla 7.- Amenazas respecto a los servicios

N°	**Código**	**Amenaza**	**Dimensión de la afectación**
Activos: Sistema web, IVR, Servicio Integrador SMS, Sistema de Monitoreo de Servicios			**Integridad [I]** **Disponibilidad [D]** **Confidencialidad [C]**
1	[E.2]	Errores del administrador	[I], [D], [C]
2	[E.15]	Alteración accidental de la información	[I]

N°	**Código**	**Amenaza**	**Dimensión de la afectación**
3	[E.18]	Destrucción de la información	[D]
4	[E.19]	Fugas de información	[C]
5	[E.24]	Caída del sistema por agotamiento de recursos	[D]
6	[A.5]	Suplantación de identidad de usuario	[I], [D], [C]
7	[A.6]	Abusos de privilegios de acceso	[I], [D], [C]
8	[A.7]	Uso no previsto	[I], [D], [C]
9	[A.11]	Acceso no autorizado	[I], [C]
10	[A.15]	Modificación deliberada de la información	[I]
11	[A.18]	Destrucción de la información	[D]
12	[A.19]	Divulgación de la información	[C]
13	[A.24]	Denegación de servicio	[D]

Fuente: elaborado por el autor de la Investigación

3.2.1.2.3. Aplicaciones informáticas – software

Tabla 8.-Amenazas respecto a las aplicaciones informáticas y software

N°	**Código**	**Amenaza**	**Dimensión de la afectación**
Activo: Sistema de soporte y asistencia técnica			**Integridad [I]** **Disponibilidad [D]** **Confidencialidad [C]**
1	[E.1]	Errores de usuario	[I], [D], [C]
2	[E.2]	Errores de administrador	[I], [D], [C]
3	[E.8]	Difusión de software dañino	[I], [D], [C]
4	[E.15]	Alteración accidental de la información	[I]
5	[E.18]	Destrucción de la información	[D]
6	[E.19]	Fugas de información	[C]
7	[A.5]	Suplantación de identidad de usuario	[I], [D], [C]
8	[A.6]	Abusos de privilegios de acceso	[I], [D], [C]
9	[A.11]	Acceso no autorizado	[I], [C]

N°	Código	Amenaza	Dimensión de la afectación
10	[A.15]	Modificación deliberada de la información	[I]
11	[A.18]	Destrucción de la información	[D]
12	[A.19]	Divulgación de la información	[C]

Fuente: elaborado por el autor de la investigación

3.2.1.2.4. Equipos Informáticos – Hardware

Tabla 9.-Amenazas a los equipos informáticos - hardware

Activos: Computadoras			
N°	**Código**	**Amenaza**	**Dimensión de la afectación** **Integridad [I]** **Disponibilidad [D]** **Confidencialidad [C]**
1	[N.1]	Fuego	[D]
2	[N.*]	Desastres naturales	[D]
3	[I.5]	Avería de origen físico o lógico	[D]
4	[E.1]	Errores de usuarios	[I], [D], [C]
5	[E.2]	Errores de administración	[I], [D], [C]
6	[E.23]	Errores de mantenimiento – actualización	[D]
7	[E.24]	Caída del sistema por agotamiento de recurso	[D]
8	[A.11]	Acceso no autorizado	[I], [C]

Fuente: elaborado por el autor de la investigación

3.2.1.2.5. Redes de comunicaciones

Tabla 10.- Amenazas a las redes de comunicaciones

N°	**Código**	**Amenaza**	**Dimensión de la afectación**
Activos: Red de comunicaciones del MDI			**Integridad [I]** **Disponibilidad [D]** **Confidencialidad [C]**
1	[E.2]	Errores del administrador	[I], [D], [C]
2	[E.19]	Fugas de información	[C]

N°	Código	Amenaza	Dimensión de la afectación
3	[E.24]	Caída del sistema por agotamiento de recursos	[D]
4	[A.12]	Análisis de tráfico	[C]
5	[A.14]	Intercepción de la información	[C]
6	[A.24]	Denegación de servicios	[D]

Fuente: elaborado por el autor de la Investigación

3.2.1.2.6. Instalaciones

Tabla 11.- Amenazas a las instalaciones

Activos: Oficina Técnica Administrativa, Oficina Dirección Nacional de Policía Comunitaria, Oficina de la UPC (Unidad de Policía Comunitaria)

N°	Código	Amenaza	Dimensión de la afectación Integridad [I] Disponibilidad [D] Confidencialidad [C]
1	[N.1]	Fuego	[D]
2	[N.*]	Desastres naturales	[D]
3	[E.15]	Alteración accidental de la información	[I]
4	[E.18]	Destrucción de la información	[D]
5	[E.19]	Fuga de información	[C]
6	[A.11]	Acceso no autorizado	[I], [C]
7	[A.15]	Modificación deliberada de la información	[I]
8	[A.18]	Destrucción de la información	[D]
9	[A.19]	Divulgación de la información	[C]

Fuente: elaborado por el autor de la Investigación

3.2.1.2.7. Las personas

Tabla 12.- Amenazas – Recurso Humano

Activos: Recurso Humano – Las personas			
N°	**Código**	**Amenaza**	**Dimensión de la afectación** **Integridad [I]** **Disponibilidad [D]** **Confidencialidad [C]**
1	[E.7]	Deficiencias en la organización	[D]
2	[E.28]	Indisponibilidad del personal	[D]
3	[A.19]	Divulgación de la información	[I], [D], [C]
4	[A.30]	Ingeniería Social	[I], [D], [C]

Fuente: elaborado por el autor de la investigación

Las tablas de la 6 hasta la 12, presentan las amenazas a las cuales están expuestos cada uno de los activos del Sistema de Botones de Seguridad y la afectación en relación a su integridad, disponibilidad y/o confidencialidad.

3.2.1.3. Estimar el impacto

La estimación del impacto se determinada por la valoración y la degradación de los activos.

Para determinar la degradación del activo, será necesario plantearse la siguiente interrogante relacionada a la afectación que tendrá un activo por la presencia de una amenaza: ***¿En caso de presentarse la (amenaza), que nivel de degradación tendría el activo?***

- ✓ ***Alta (A)***
- ✓ ***Media (M)***
- ✓ ***Baja (B)***

La degradación se analiza para cada una de las amenazas y cada uno de los activos determinados en los pasos anteriores; en Tabla 13 Matriz de valoración del impacto sobre los activos se muestra la "Degradación" valorada.

Una vez determinada la degradación y con los valores encontrados en la Tabla 4. Valoración de los activos de acuerdo a su criticidad, ya será posible estimar el impacto que puede producir la materialización de una amenaza. Para esta valoración se utilizará la Figura 3, la cual establece los valores cualitativos del impacto de acuerdo al valor del activo y a su degradación.

Los resultados obtenidos pueden visualizarse en la siguiente tabla:

Tabla 13 .- Valoración del impacto sobre los activos

Activo	**Código**	**Amenaza**	**Vulnerabilidad**	**Valoración Activo**	**Degradación Activo**	**Impacto**
Datos – Información: Base de datos Registros: ciudadanos, policías, alarmas o eventos atendidos y reportes de SMS	[E.1]	Errores de usuarios	Falta de manuales de usuario	MA	B	M
	[E.2]	Errores del administrador	Falta de manuales de usuario y manuales de procesos	MA	M	A
	[E.15]	Alteración accidental de la información	Falta de controles en los procesos de modificación	MA	A	MA
	[E.18]	Destrucción de la información	Falta de controles en los procesos de eliminación	MA	A	MA
	[E.19]	Fugas de información	Falta de controles en la asignación de perfiles de usuario	MA	A	MA
	[A.6]	Abusos de privilegio de acceso	Falta de registros de control en el acceso a la información	MA	A	MA
	[A.11]	Acceso no autorizado	Contraseñas débiles	MA	A	MA
	[A.15]	Modificación deliberada de la información	Falta de control en los procesos de desvinculación de los empleados	MA	A	MA
	[A.18]	Destrucción de la información	Falta de control en las cuentas dadas de baja	MA	A	MA
	[A.19]	Divulgación de la información	Falta de control en las cuentas dadas de baja	MA	M	A
Servicios: Sistema web, IVR, Servicio Integrador SMS,	[E.2]	Errores del administrador	Falta de manuales de usuario y manuales de procesos	MA	M	A
	[E.15]	Alteración accidental de la	Falta de controles en los	MA	A	MA

Activo	Código	Amenaza	Vulnerabilidad	Valoración Activo	Degradación Activo	Impacto
Sistema de Monitoreo de Servicios		información	procesos de modificación			
	[E.18]	Destrucción de la información	Falta de controles en los procesos de eliminación	MA	A	MA
	[E.19]	Fugas de información	Falta de controles en la asignación de perfiles de usuario	MA	A	MA
	[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	MA	A	MA
	[A.5]	Suplantación de identidad de usuario	Contraseñas débiles o predecibles	MA	A	MA
	[A.6]	Abusos de privilegios de acceso	Falta de registros de control en el acceso a los servicios	MA	A	MA
	[A.7]	Uso no previsto	Falta de registros de control en el acceso a los servicios	MA	A	MA
	[A.11]	Acceso no autorizado	Contraseñas inseguras	MA	A	MA
	[A.15]	Modificación deliberada de la información	Contraseñas inseguras	MA	A	MA
	[A.18]	Destrucción de la información	Falta de control en las cuentas dadas de baja	MA	A	MA
	[A.19]	Divulgación de la información	Falta de suscripción de acuerdos de confidencialidad	MA	A	MA
	[A.24]	Denegación de servicio	Saturación de recursos tecnológicos	MA	A	MA
Aplicaciones informáticas – software: Sistema de Soporte y asistencia técnica	[E.1]	Errores de usuario	Falta de manuales de usuario	M	M	B
	[E.2]	Errores de administrador	Falta de manuales de usuario y manuales procesos	M	A	M
	[E.8]	Difusión de software dañino	Virus y demás software malicioso	M	M	B

Activo	Código	Amenaza	Vulnerabilidad	Valoración Activo	Degradación Activo	Impacto
	[E.15]	Alteración accidental de la información	Falta de control en los procesos de modificación	M	A	M
	[E.18]	Destrucción de la información	Falta de control en los procesos de eliminación	M	A	M
	[E.19]	Fugas de información	Falta de controles en la asignación de perfiles de usuario	M	B	MB
	[A.5]	Suplantación de identidad de usuario	Contraseñas inseguras o predecibles	M	M	B
	[A.6]	Abusos de privilegios de acceso	Falta de registros de control en el acceso a los sistemas	M	M	B
	[A.11]	Acceso no autorizado	Contraseñas inseguras	M	M	B
	[A.15]	Modificación deliberada de la información	Falta de control en los procesos de desvinculación de los empleados	M	A	M
	[A.18]	Destrucción de la información	Falta de control en las cuentas dadas de baja	M	A	M
	[A.19]	Divulgación de la información	Falta de suscripción de acuerdos de confidencialidad	M	M	B
Equipos informáticos – Hardware: Computadoras	[N.1]	Fuego	No se ha socialización como usar los extintores	A	M	M
	[N.*]	Desastres naturales		A	M	M
	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	A	M	M
	[E.1]	Errores de usuarios	Desconocimiento del uso de computadoras	A	B	B
	[E.23]	Errores de mantenimiento – actualización	Falta de procesos de actualización y mantenimiento	A	B	B
	[E.24]	Caída del sistema por	Desconocimiento del uso de	A	B	B

Activo	Código	Amenaza	Vulnerabilidad	Valoración Activo	Degradación Activo	Impacto
		agotamiento de recursos	computadoras			
	[A.11]	Acceso no autorizado	Equipos sin contraseñas	A	M	M
Redes de comunicaciones: Red de comunicaciones del MDI	[E.2]	Errores del administrador	Falta de manuales de usuario y manuales procesos	MA	M	A
	[E.19]	Fugas de información	Puertos abiertos innecesariamente	MA	M	A
	[E.24]	Caída del sistema por agotamiento de recursos	Falta de control en el uso de la red	MA	M	A
	[A.12]	Análisis de tráfico	Puertos abiertos innecesariamente	MA	M	A
	[A.14]	Intercepción de la información	Puertos abiertos innecesariamente	MA	A	MA
	[A.24]	Denegación de servicios	Puertos abiertos innecesariamente, controles no adecuados n el firewall de la red	MA	M	M
Instalaciones: Oficina Técnica Administrativa, Oficina Dirección Nacional de Policía Comunitaria, Oficina de la UPC (Unidad de Policía Comunitaria)	[N.1]	Fuego	No se ha socialización como usar los extintores	M	M	B
	[N.*]	Desastres naturales		M	M	B
	[E.15]	Alteración accidental de la información	Falta de controles en el acceso físico	M	A	M
	[E.18]	Destrucción de la información	Falta de controles en el acceso físico	M	A	M
	[E.19]	Fuga de información	Falta de controles en el acceso físico	M	M	B
	[A.11]	Acceso no autorizado	Falta de controles en el acceso físico	M	M	B
	[A.15]	Modificación deliberada de la información	La información física no se encuentra en un lugar bajo	M	A	M

Activo	Código	Amenaza	Vulnerabilidad	Valoración Activo	Degradación Activo	Impacto
			llave			
	[A.18]	Destrucción de la información	La información física no se encuentra en un lugar bajo llave	M	A	M
	[A.19]	Divulgación de la información	La información física no se encuentra en un lugar bajo llave	M	M	B
Las personas: Recurso humano	[E.7]	Deficiencias en la organización	Falta de asignación de roles y responsabilidades	MA	A	MA
	[E.28]	Indisponibilidad del personal	Falta de transferencia de conocimientos	MA	A	MA
	[A.19]	Divulgación de la información	Falta de procesos en la desvinculación del personal	MA	A	MA
	[A.30]	Ingeniería Social	Falta de conocimiento de la seguridad de la información	MA	A	MA

Fuente: elaborado por el autor de la investigación

3.2.1.4. Estimación del Riesgo

El siguiente paso de acuerdo a la Metodología de Magerit es estimar el riesgo, el cual se determina entre la combinación del impacto y la frecuencia de ocurrencia.

La probabilidad de ocurrencia tiene relación a la frecuencia de ocurrencia en la que se puede presentar la amenaza:

- ✓ Muy frecuente
- ✓ Frecuente
- ✓ Normal
- ✓ Poco frecuente
- ✓ Muy poco frecuente

Los valores cualitativos descritos en la Figura 4, permite determinar la probabilidad de ocurrencia de una amenaza. La probabilidad se encuentra determinada en la columna "Probabilidad" del Anexo 3.

Finalmente con la probabilidad y el impacto, será posible estimar el riesgo. La figura 5, permite estimar de forma cualitativa el riesgo a través del impacto y la probabilidad de ocurrencia.

El impacto, la probabilidad y el riesgo queda valorado cualitativamente de la siguiente manera:

IMPACTO	PROBABILIDAD	RIESGO
MA: Muy alto	MA: Prácticamente seguro	MA: Crítico
A:Alto	A: Probable	A:Importante
M: Medio	M: Posible	M: Apreciable
B: Bajo	B: Poco probable	B: Bajo
MB: Muy bajo	MB: Muy raro	MB: Despreciable

Figura 12.- Impacto, probabilidad y riesgo
Fuente: (Ministerio de Hacienda y Administraciones Públicas 2012, pág. 7)

3.2.1.5. Determinar las salvaguardas frente al riesgo

Finalmente las salvaguardas o controles que se apliquen, pretenden minimizar la probabilidad de ocurrencia de la amenaza.

Para la selección de los controles, se ha tomado la Norma ISO/IEC 27002:2013; estos controles han sido escogidos en base a los activos, amenazas y vulnerabilidades determinadas en los pasos anteriores. En la Tabla 14 se detallan los controles seleccionados.

De acuerdo a los controles seleccionados, se irá desarrollando la Política de Seguridad de la Información.

Tabla 14.- Matriz de riesgos y Controles ISO/IEC 27002:2013

Activo	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Prob.**	**Riesgo**	**Control**
Datos – Información: Base de datos Registros: ciudadanos, policías, alarmas o eventos atendidos y reportes de SMS	[E.1]	Errores de usuarios	Falta de manuales de usuario	M	A	A	12.1.1 Documentación de procedimientos de operación
	[E.2]	Errores del administrador	Falta de manuales de usuario y manuales de procesos	A	M	A	12.1.1 Documentación de procedimientos de operación
	[E.15]	Alteración accidental de la información	Falta de controles en los procesos de modificación	MA	M	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[E.18]	Destrucción de la información	Falta de controles en los procesos de eliminación	MA	B	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[E.19]	Fugas de información	Falta de controles en la asignación de perfiles de usuario	MA	M	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[A.6]	Abusos de privilegio de acceso	Falta de registros de control en el acceso a la información	MA	B	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[A.11]	Acceso no autorizado	Contraseñas débiles	MA	M	MA	9.2.3 Gestión de contraseñas de usuarios
	[A.15]	Modificación deliberada de la información	Falta de control en los procesos de desvinculación de los empleados	MA	B	MA	9.2.6 Retirada o adaptación de los derechos de acceso
	[A.18]	Destrucción de la información	Falta de control en las cuentas dadas de baja	MA	B	MA	9.2.6 Retirada o adaptación de los derechos de acceso
	[A.19]	Divulgación de la información	Falta de control en las cuentas dadas de baja	A	M	A	9.2.6 Retirada o adaptación de los derechos de acceso
	[E.2]	Errores del	Falta de manuales de	A	M	A	12.1.1 Documentación

Activo	Código	Amenaza	Vulnerabilidad	Impacto	Prob.	Riesgo	Control
		administrador	usuario y manuales de procesos				de procedimientos de operación
Servicios: Sistema web, IVR, Servicio Integrador SMS, Sistema de Monitoreo de Servicios	[E.15]	Alteración accidental de la información	Falta de controles en los procesos de modificación	MA	M	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[E.18]	Destrucción de la información	Falta de controles en los procesos de eliminación	MA	B	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[E.19]	Fugas de información	Falta de controles en la asignación de perfiles de usuario	MA	M	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	MA	M	MA	12.1.3 Gestión de capacidades 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores 15.2.1 Supervisión y revisión de los servicios prestados por terceros 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información
	[A.5]	Suplantación de identidad de usuario	Contraseñas débiles o predecibles	MA	M	MA	9.2.3 Gestión de contraseñas de usuarios
	[A.6]	Abusos de privilegios de acceso	Falta de registros de control en el acceso a los servicios	MA	M	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales 9.3.1 Uso de información confidencial para la

Activo	Código	Amenaza	Vulnerabilidad	Impacto	Prob.	Riesgo	Control
							autenticación
	[A.7]	Uso no previsto	Falta de registros de control en el acceso a los servicios	MA	M	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[A.11]	Acceso no autorizado	Contraseñas inseguras	MA	M	MA	9.2.3 Gestión de contraseñas de usuarios
	[A.15]	Modificación deliberada de la información	Contraseñas inseguras	MA	B	MA	9.2.3 Gestión de contraseñas de usuarios 16.1.2 Notificación de eventos de seguridad de la información
	[A.18]	Destrucción de la información	Falta de control en las cuentas dadas de baja	MA	MB	A	9.2.6 Retirada o adaptación de los derechos de acceso 16.1.2 Notificación de eventos de seguridad de la información
	[A.19]	Divulgación de la información	Falta de control en las cuentas dadas de baja	MA	M	MA	9.2.6 Retirada o adaptación de los derechos de acceso 16.1.2 Notificación de eventos de seguridad de la información
	[A.24]	Denegación de servicio	Saturación de recursos tecnológicos	MA	M	MA	12.1.3 Gestión de capacidades
Aplicaciones informáticas – software: Sistema de Soporte y asistencia técnica	[E.1]	Errores de usuario	Falta de manuales de usuario	B	A	M	12.1.1 Documentación de procedimientos de operación
	[E.2]	Errores de administrador	Falta de manuales de usuario y manuales procesos	M	M	M	12.1.1 Documentación de procedimientos de operación
	[E.8]	Difusión de	Virus y demás software	B	A	M	12.2.1 Controles contra

Activo	Código	Amenaza	Vulnerabilidad	Impacto	Prob.	Riesgo	Control
		software dañino	malicioso				el código malicioso
	[E.15]	Alteración accidental de la información	Falta de control en los procesos de modificación	M	M	M	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[E.18]	Destrucción de la información	Falta de control en los procesos de eliminación	M	B	M	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[E.19]	Fugas de información	Falta de controles en la asignación de perfiles de usuario	MB	B	MB	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[A.5]	Suplantación de identidad de usuario	Contraseñas inseguras o predecibles	B	M	B	9.4.3 Gestión de contraseñas de usuario
	[A.6]	Abusos de privilegios de acceso	Falta de registros de control en el acceso a los sistemas	B	M	B	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[A.11]	Acceso no autorizado	Contraseñas inseguras	B	M	B	9.2.3 Gestión de contraseñas de usuarios
	[A.15]	Modificación deliberada de la información	Falta de control en los procesos de desvinculación de los empleados	M	B	M	9.2.6 Retirada o adaptación de los derechos de acceso
	[A.18]	Destrucción de la información	Falta de control en los procesos de desvinculación de los empleados	M	B	M	9.2.6 Retirada o adaptación de los derechos de acceso
	[A.19]	Divulgación de la información	Falta de suscripción de acuerdos de confidencialidad	B	M	B	13.2.4 Acuerdos de confidencialidad y secreto
Equipos informáticos – Hardware:	[N.1]	Fuego	No se ha socialización como usar los extintores	M	MB	B	11.1.4 Protección contra las amenazas externas y ambientales
Computadoras	[N.*]	Desastres naturales		M	MB	B	11.1.4 Protección

Activo	Código	Amenaza	Vulnerabilidad	Impacto	Prob.	Riesgo	Control
							contra las amenazas externas y ambientales
	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	M	M	M	11.2.4 Mantenimiento de los equipos
	[E.1]	Errores de usuarios	Desconocimiento del uso de computadoras	B	A	M	12.1.1 Documentación de procedimientos de operación
	[E.23]	Errores de mantenimiento - actualización	Falta de procesos de actualización y mantenimiento	B	M	B	11.2.4 Mantenimiento de los equipos
	[E.24]	Caída del sistema por agotamiento de recursos	Desconocimiento del uso de computadoras	B	M	B	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla
	[A.11]	Acceso no autorizado	Equipos sin contraseñas	M	M	M	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla
Redes de comunicaciones: Red de comunicaciones del MDI	[E.2]	Errores del administrador	Falta de manuales de usuario y manuales procesos	A	M	A	12.1.1 Documentación de procedimientos de operación
	[E.19]	Fugas de información	Puertos abiertos innecesariamente	A	M	A	13.1.2 Mecanismos de seguridad asociados a servicios de red
	[E.24]	Caída del sistema por agotamiento de recursos	Falta de control en el uso de la red	A	M	A	12.1.3 Gestión de capacidades
	[A.12]	Análisis de tráfico	Puertos abiertos innecesariamente	A	M	A	13.1.2 Mecanismos de seguridad asociados a servicios de red
	[A.14]	Intercepción de la información	Puertos abiertos innecesariamente	MA	M	MA	13.1.2 Mecanismos de seguridad asociados a

Activo	Código	Amenaza	Vulnerabilidad	Impacto	Prob.	Riesgo	Control
							servicios de red
	[A.24]	Denegación de servicios	Puertos abiertos innecesariamente, controles no adecuados en el firewall de la red	M	M	M	13.1.2 Mecanismos de seguridad asociados a servicios de red
Instalaciones: Oficina Técnica Administrativa, Oficina Dirección Nacional de Policía Comunitaria, Oficina de la UPC (Unidad de Policía Comunitaria)	[N.1]	Fuego	No se ha socialización como usar los extintores	B	B	B	11.1.4 Protección contra las amenazas externas y ambientales
	[N.*]	Desastres naturales		B	B	B	11.1.4 Protección contra las amenazas externas y ambientales
	[E.15]	Alteración accidental de la información	Falta de controles en el acceso físico	M	B	M	11.1.2 Controles físicos de entrada
	[E.18]	Destrucción de la información	Falta de controles en el acceso físico	M	B	M	11.1.2 Controles físicos de entrada
	[E.19]	Fuga de información	Falta de controles en el acceso físico	B	B	B	11.1.2 Controles físicos de entrada
	[A.11]	Acceso no autorizado	Falta de controles en el acceso físico	B	M	B	11.1.2 Controles físicos de entrada
	[A.15]	Modificación deliberada de la información	La información física no se encuentra en un lugar bajo llave	M	B	M	11.1.2 Controles físicos de entrada
	[A.18]	Destrucción de la información	La información física no se encuentra en un lugar bajo llave	M	MB	B	11.1.2 Controles físicos de entrada
	[A.19]	Divulgación de la información	La información física no se encuentra en un lugar bajo llave	B	M	B	11.1.2 Controles físicos de entrada
Las personas: Recurso humano	[E.7]	Deficiencias en la organización	Falta de asignación de roles y responsabilidades	MA	M	MA	6.1.1 Asignación de responsabilidades para

Activo	Código	Amenaza	Vulnerabilidad	Impacto	Prob.	Riesgo	Control
							la seguridad de la información
	[E.28]	Indisponibilidad del personal	Falta de transferencia de conocimientos	MA	M	MA	7.2.2 Concienciación, educación y capacitación en seguridad de la información
	[A.19]	Divulgación de la información	Falta de procesos en la desvinculación del personal	MA	M	MA	7.2.3 Proceso disciplinario 13.2.4 Acuerdos de confidencialidad y secreto 13.2.2 Acuerdos de intercambio 7.3.1 Cese o cambio de puesto de trabajo
	[A.30]	Ingeniería Social	Falta de conocimiento de la seguridad de la información	MA	A	MA	7.2.2 Concienciación, educación y capacitación en seguridad de la información

Fuente: elaborado por el autor de la investigación

CAPÍTULO IV

PROPUESTA

A continuación se presenta la propuesta de la Política de Seguridad de la información basada en la norma NTE INEN ISO/IEC 27002:2013, para el Sistema de Botones de Seguridad del Ministerio del Interior.

4.1. OBJETO Y CAMPO DE APLICACIÓN

La Política de Seguridad de la Información establece las directrices y normativas que se aplicará al Sistema de Botones de Seguridad del Ministerio del Interior y los funcionarios que forman parte de este Sistema Integral de Seguridad.

4.2. REFERENCIAS NORMATIVAS

- ✓ El presente documento está basado en la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002:2013; traducción idéntica de la Norma Internacional ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls.*

4.3. TÉRMINOS Y DEFINICIONES

- ✓ **Seguridad de la información.-** es la disciplina que abarca los sistemas de protección física, la prevención de accidentes o la prevención de actividades desleales por parte de los empleados de una organización o empresa (Gómez, 2007, pág. 3).

- ✓ **Confidencialidad.-** hace referencia a la privacidad de la información almacenada y que se procesa dentro de un sistema informático; bajo este principio, las herramientas de seguridad deben proteger el sistema de intrusos y accesos de personas o programas no autorizados.
- ✓ **Integridad.-** hace referencia a la validez y consistencia de la información almacenada, las herramientas de seguridad deben asegurar que los procesos de actualización estén sincronizados a fin de evitar la duplicidad de la información.
- ✓ **Disponibilidad.-** hace referencia a la continuidad de acceso a la información almacenada y procesada dentro de un sistema informático; bajo este principio, las herramientas de seguridad, deben contribuir a la permanencia de la información en un sistema.
- ✓ **Riesgo.-** el riesgo se define como la probabilidad de que se materialice o no una amenaza, debido a la presencia de vulnerabilidades existentes en un sistema informático o su entorno (Aguilera, 2010, pág. 14).
- ✓ **Ataque.-** Se produce un ataque accidental o deliberadlo cuando se ha materializado una amenaza en contra de un activo.
- ✓ **Vulnerabilidad.-** es una debilidad la cual puede ser aprovechada por una o varias amenazas para causar daños sobre un activo o sobre una organización.
- ✓ **Incidente de seguridad.**- suceso imprevisto y no sedeado que atenta a la integridad, disponibilidad o confidencialidad de la información.

4.4. ABRVIATURAS

- ✓ **ID:** Identificador de usuario
- ✓ **IEC:** Comisión Internacional de Electrotécnica

- ✓ **ISO:** Organización Internacional de Normalización
- ✓ **IVR:** Respuesta de vos interactiva
- ✓ **LOSEP:** Ley Orgánica de Servicio Público
- ✓ **MDI:** Ministerio del Interior
- ✓ **SLA:** Acuerdo de Nivel de Servicio
- ✓ **SMS:** Servicio de mensajes simple
- ✓ **TICs:** Tecnologías de la Información y Comunicaciones
- ✓ **UPC:** Unidad de Policía Comunitaria

4.5. POLÍTICA DE SEGURIDAD

4.5.1. OBJETIVO

Establecer las directrices y normativas destinadas a garantizar la confidencialidad, disponibilidad e integridad de la información a través de una adecuada orientación y soporte para los procesos de gestión de la seguridad de la información.

4.5.2. RESPONSABLILIDADES

- ✓ **Coordinador General de las Tecnologías de la Información. -** responsable y con autoridad para aprobar la política de seguridad, aprobar las actualizaciones realizadas y gestionar el cumplimiento de las normativas y disposiciones establecidas.
- ✓ **Máxima autoridad o su delegado.-** responsable y con autoridad para autorizar y disponer la implementación de la Política de Seguridad.
- ✓ **Oficial de Seguridad de la Información. -** realizar la revisión de los procedimientos, normativas y controles establecidos en la política de seguridad, socializar la política de seguridad aprobada y verificar el cumplimiento de la misma.

- ✓ **Funcionarios.-** conocer y aplicar las normativas establecidas en la política de seguridad.
- ✓ **Líder Metodológico de Procesos. -** responsable de la normalización del documento, acorde a los manuales de Procesos del Ministerio del Interior.

4.5.3. DESARROLLO DE LA POLÍTICA

Tabla 15.- Seguridad ligada a los recursos humanos

INSTITUCIÓN	**MINISTERIO DEL INTERIOR – SISTEMA DE BOTONES DE SEGURIDAD**
POLÍTICA	**POLÍTICA DE SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**
OBJETIVO	Asegurar que los funcionarios conozcan y cumplan con sus responsabilidades en la seguridad de la información a través de la educación preventiva.
DURANTE LA CONTRATACIÓN	
Concienciación, educación y formación en seguridad de la información	**Referencia: 7.2.2**
a. La Coordinación general de Tecnologías de la Información del MDI, deberá establecer la planificación para las capacitaciones en los temas relacionados a la seguridad de la información en el Sistema de Botones de Seguridad; estas capacitaciones deberán realizarse por lo menos dos veces al año. b. Los funcionarios responsables de la capacitación son: el Oficial de Seguridad de la Información del MDI y un funcionario conocedor de los servicios y aplicaciones de la Plataforma Tecnológica del Sistema de Botones de Seguridad, designado por el	

Coordinador General de TICs.

c. Las capacitaciones y socializaciones realizadas deberán tener su respectivo entregable o documento de respaldo, el cual deberá incluir los datos y firmas del personal capacitado y del personal capacitado.
d. Es obligación de los funcionarios que forman parte del Sistema de Seguridad Integral - Botones de Seguridad, acudir a las capacitaciones y socializaciones planificadas por la Coordinación General de TICs.
e. Durante el proceso de vinculación de un nuevo funcionario, antes de tener otorgarle cualquier tipo de acceso a un sistema o servicio de tecnológico, deberá recibir la capacitación y socialización en los temas relacionados a la seguridad de la información.
f. Es obligación de los funcionarios que forman parte del Sistema de Seguridad Integral de Botones de Seguridad, cumplir con las normativas y disposiciones contempladas en el presente documento,

Proceso Disciplinario	**Referencia: 7.2.3**

a. El proceso normativo interno disciplinario del Ministerio del Interior deberá ser socializado a los funcionarios que forman parte del Sistema de Botones de Seguridad, así como el Reglamento de Disciplina de la Policía Nacional del Ecuador, según corresponda.
b. El Oficial de Seguridad de la Información conjuntamente con un delegado de la Coordinación de General de TICs, deberán verificar si efectivamente se ha producido una violación de la seguridad.
c. El oficial de Seguridad de la Información y el delegado de la Coordinación General de

TICs, deberán elaborar un informe referente a lo sucedido, dicho informe deberá ser objetivo e imparcial.

d. El Coordinador General de TICs deberá remitir de manera formal a la Dirección de Talento Humano el informe referente al evento sucedido, para el análisis correspondiente.
e. Las sanciones o procesos disciplinarios estarán sujetos al Artículo 42 "*De las faltas disciplinarias"* y Artículo 43 *"Sanciones disciplinarias"* de la Ley Orgánica del Servicio Público LOSEP; Reglamento Interno de Administración de Talento Humano del Ministerio del Interior y el Reglamento de Disciplina de la Policía Nacional del Ecuador; según corresponda.

CESE O CAMBIO DE PUESTO DE TRABAJO

Cese o cambio de puesto de trabajo	**Referencia: 7.3.1**

a. La Coordinación General de TICs del Ministerio del Interior, deberá solicitar a la Dirección de Talento Humano del MDI, que se incluya en el "Acta de Paz y Salvo", la firma de verificación de dada de baja de cuentas asociadas a los servicios tecnológicos del Sistema de Botones de Seguridad.
b. La Coordinación General de TICs del MDI, deberá designar de manera formal, un delegado del Sistema de Botones de Seguridad, responsable del retiro o dada de baja de las cuentas y perfiles de usuario, además será el responsable de la firma del Acta de Paz y Salvo correspondiente.
c. La Coordinación de la Dirección Nacional de Policía Comunitaria, deberá dar a conocer a la Coordinación General de TICs, los procesos de desvinculación o cambio de funciones de los Jefes y Coordinadores de Policía Comunitaria a nivel nacional.

d. La entrega de computadoras y demás activos deberán seguir el procedimiento establecido por la Unidad de Bienes del MDI para la entrega o traspaso de los mismos.

Elaborado por: autor de la Investigación

Tabla 16.- Control de accesos

INSTITUCIÓN	**MINISTERIO DEL INTERIOR – SISTEMA DE BOTONES DE SEGURIDAD**
POLÍTICA	**POLÍTICA PARA EL CONTROL DE ACCESOS**
OBJETIVO	Limitar el acceso a la información y a las instalaciones de procesamiento de datos e información del Sistema de Botones de Seguridad.
GESTIÓN DE ACCESO A USUARIOS	
Gestión de los derechos de acceso con privilegios especiales	**Referencia: 9.2.3**
a. Los requerimientos de cuentas de usuario para el acceso al sistema Web de Botones de Seguridad deberán ser analizados previo a su entrega; el análisis deberá basarse en la función que desempeñará el usuario y privilegios necesarios. Se deberá tomar en cuenta las siguientes consideraciones para la asignación del perfil de usuario:	

Privilegios / Necesidades						Perfil de usuario
Registro	**Modificación**	**Eliminación**	**Monitoreo**	**Reportería**	**Cierre alarmas**	
X	X		X	X	X	Operador
			X	X		Distrito
			X	X		Inspector
X	X	X	X	X		Supervisor
X	X	X	X	X	X	Administrador

b. El Coordinador General de TICs, será quien apruebe la asignación y entrega de un perfil de usuario del Sistema Web de Botones de Seguridad.

c. Se debe revisar de manera semestral las competencias de los usuarios asignados con perfiles de supervisión y administración.

Retirada o adaptación de los derechos de acceso	**Referencia: 9.2.6**

a. La Dirección de Talento Humano del MDI debe notificar a la Coordinación General de TICs del MDI la terminación de contratos o cambios de funciones de los funcionarios asociados a la Unidad Técnica Administrativa del Sistema de Botones de Seguridad.

b. La Coordinación de la Dirección Nacional de Policía Comunitaria, deberá dar a conocer a la Coordinación General de TICs, los procesos de desvinculación o cambio de funciones de los Jefes y Coordinadores de Policía Comunitaria a nivel nacional.

c. La Coordinación General del TICs deberá disponer de manera inmediata según sea el caso el retiro o ajuste (privilegios) de acceso a las cuentas de usuario de los recursos tecnológicos del sistema de Botones de Seguridad.

RESPONSABILIDADES DEL USUARIO	
Uso de información confidencial para la autenticación	**Referencia: 9.3.1**

a. Los funcionarios son responsables de mantener la confidencialidad de sus contraseñas, estas son personales e intransferibles.
b. Las contraseñas de acceso a cualquier servicio de la plataforma tecnológica de Botones de Seguridad, no deberán ser almacenadas en agendas, hojas ni en ficheros o archivos de software que no tengan características de repositorios seguros de contraseñas.
c. Las contraseñas utilizadas para acceso a la plataforma tecnológica del Sistema de Botones de Seguridad no deberán estar asociadas a las contraseñas de tipo personal de los usuarios.

CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	
Gestión de contraseñas de usuario	**Referencia: 9.4.3**

a. Las cuentas de usuario asignadas a los perfiles: Distrito, Inspector, Supervisor y Administrador del Sistema web de botones de Seguridad, deberán mantener un identificador (ID) de usuario y contraseñas individuales, este principio permitirá mantener la responsabilidad.
b. Las cuentas de usuario del Sistema Web de Botones de Seguridad, deberán permitir a todos los usuarios, definir sus propias contraseñas.
c. Las contraseñas de acceso a cualquier perfil o entorno del sistema web de Botones de Seguridad, deberán contener al mínimo 10 caracteres, obligatoriamente deberán estar formados por letras mayúsculas y minúsculas, números y al menos un caracter especial.

d. Al inicio de sesión de una nueva cuenta de usuario del sistema web de Botones de Seguridad, este deberá solicitar el cambio de contraseña de manera obligatoria.
e. Se deberá establecer un proceso que forcé al cambio de contraseña de las cuentas de acceso al Sistema Web de Botones de Seguridad, este proceso deberá realizarse con una periodicidad de 6 meses.
f. Los entornos o pantallas de ingreso a cualquier entorno o perfil de usuario del sistema web de Botones de Seguridad, no deberán mostrar las contraseñas digitadas por los usuarios.
g. Los archivos que mantengan las contraseñas de las cuentas de usuario deberán estar cifrados y protegidos.

Elaborado por: autor de la Investigación

Tabla 17.- Seguridad física y ambiental

INSTITUCIÓN	**MINISTERIO DEL INTERIOR – SISTEMA DE BOTONES DE SEGURIDAD**
POLÍTICA	**SEGURIDAD FÍSICA Y AMBIENTAL**
OBJETIVO	Prevenir y controlar el acceso físico no autorizado, daños y demás vulnerabilidades que pongan en riesgo a la información y a las instalaciones de procesamiento de información del Sistema de Botones de Seguridad.
AREAS SEGURAS	
Controles físicos de entrada	**Referencia:11.1.2**
a. El personal de seguridad responsable de la entrada principal del Ministerio del Interior deberá controlar el acceso de personas externas a la institución, para dicho efecto deberá	

registrar en la bitácora la fecha y hora de ingreso y salida de las personas, así como permitir el acceso únicamente bajo autorización y con conocimiento del propósito de ingreso.

b. Las personas externan que deseen ingresar a la institución deberán obligatoriamente presentar un documento de identificación como la cédula de identidad o una credencial de identificación.
c. Se debe entregar a los visitantes una credencial de identificación de "Visitante", la misma que debe indicar el piso o dependencia en la cual tiene autorización a ingresar.
d. Si el personal que ingresa porta una computadora, esta deberá ser registrada con los datos de su marca, modelo y número de serie.
e. Los visitantes deberán ser revisados a la entrada y a la salida de las instalaciones del Ministerio del Interior.
f. El acceso a la oficina Técnica Administrativa del Sistema de Botones de Seguridad deberá permitirse únicamente a personal autorizado,

Protección contra las amenazas externas y ambientales	**Referencia:11.1.4**

a. La Coordinación General de TICs deberá solicitar a la Unidad de Gestión de Riesgos del MDI, se imparta capacitaciones relacionadas a las maneras de evitar daños causados por riesgos naturales como inundaciones, terremotos, explosiones y otras amenazas ocasionadas por desastres naturales o por el hombre.
b. La coordinación general de Tics deberá delegar al personal que forme parte de la Brigada de Gestión de Riesgos del MDI quienes deberán capacitarse en los protocolos y procedimientos para actuar ante las amenazas descritas anteriormente.

SEGURIDAD DE LOS EQUIPOS	
Mantenimiento de los equipos	**Referencia:11.2.4**

a. La Coordinación General de TICs de MDI deberá disponer a la Unidad de Soporte Técnico del MDI establecer el plan de mantenimiento de equipos de las diferentes unidades administrativas del MDI en la cual deberá incluirse la Unidad Técnica Administrativa del Sistema de Botones de Seguridad.
b. Únicamente el personal de la Unidad de soporte Técnico del MDI, podrá realizar la reparación y mantenimiento de los equipos.
c. Se deberá mantener los registros de fallas en los equipos además se deberá registrar los planes de mantenimiento preventivos y correctivos realizados.
d. Los mantenimientos a realizarse sobre los equipos deberán basarse en las especificaciones y recomendaciones establecidas por los fabricantes.

Política de puesto de trabajo despejado y bloqueo de pantalla	**Referencia:11.2.9**

Los siguientes procedimientos, excluyen a las computadoras que se encuentran en las Unidades de Policía Comunitaria (UPC).

a. Los Cds, discos duros y demás medios de almacenamiento que contienen información referente a los registros de ciudadanos en el sistema de Botones de Seguridad, deberán estar guardados en archivadores o muebles seguros y bajo llave.
b. Es obligación de los funcionarios bloquear las computadoras cuando no se encuentren en su sitio de trabajo.
c. Las computadoras de los funcionarios deben configurarse, de tal manera que si no existe

actividad en la misma, se bloquee de forma automática en el transcurso de un minuto.

d. Todas las computadoras de los funcionarios deberán tener una clave o contraseña de protección para acceder a la misma.

e. Al terminar la jornada de trabajo, las computadoras deberán apagarse.

Elaborado por: autor de la Investigación

Tabla 18.- Seguridad en las operaciones

INSTITUCIÓN	**MINISTERIO DEL INTERIOR – SISTEMA DE BOTONES DE SEGURIDAD**
POLÍTICA	**POLÍTICA DE SEGURIDAD EN LAS OPERACIONES**
OBJETIVO	Asegurar la correcta operatividad y procesamiento de la información en el Sistema de Botones de Seguridad.
RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN	
Documentos de procedimientos de operación	**Referencia:12.1.1**

a. La Unidad técnica administrativa deberá elaborar los manuales de usuario del sistema web de Botones de Seguridad para todos los perfiles de usuario; sistemas de monitoreo y sistema de Reportería SMS.

b. La Unidad Técnica Administrativa deberá elaborar los manuales de procedimientos para la ejecución de pruebas y funcionalidad del servicio de IVR e integrador SMS.

c. La Unidad Técnica administrativa deberá elaborar el manual de procedimientos del monitoreo de servicios y recursos tecnológicos que forman parte del Sistema de Botones de Seguridad.

d. La Unidad Técnica Administrativa deberá elaborar el manual de procedimientos de

respuesta a las incidencias presentadas en los servicios tecnológicos del Sistema de Botones de Seguridad.

e. La Unidad Técnica Administrativa, deberá mantener actualizados y vigentes los SLA o Acuerdos de Nivel de Servicio con los proveedores de servicios tecnológicos.

Los niveles de escalamiento descritos en los SLA, deberán contener la siguiente información:

Nivel	**Tiempo máximo de escalamiento**	**Nombre del Responsable**	**Cargo**	**Correo electrónico**	**Teléfono**

Gestión de las capacidades	**Referencia: 12.1.3**

a. El administrador de la Plataforma tecnológica del Sistema de Botones de Seguridad, deberá solicitar de manera trimestral al proveedor del servicio, un informe referente al tráfico de llamadas entrantes al servicio de IVR, el análisis correspondiente permitirá determinar si el número de canales asignado a dicho servicio es el necesario.

b. Se deberá establecer un procedimiento entre la Coordinación General de TICs y la Coordinación de Policía Comunitaria a fin de realizar una depuración de la base de datos de registros ciudadanos con la finalidad de liberar espacio de almacenamiento y evitar contratar de manera innecesaria más recursos.

c. Previo a cualquier proceso de contratación de servicios o recursos tecnológicos, se deberá realizar un estudio de factibilidad técnica, este estudio deberá contener el análisis de la situación actual y el dimensionamiento o proyección de los recursos a contratarse, basado en las necesidades reales del sistema de Botones de Seguridad.

PROTECCIÓN CONTRA CÓDIGO MALICIOSO	
Controles contra el código malicioso	**Referencia: 12.2.1**
a. Se prohíbe a todos los funcionarios, la instalación de cualquier tipo de software en los computadores de la organización sin previa autorización. b. Las computadoras asignadas a los funcionarios deberán estar configuradas con perfiles de usuario restringido para la instalación de programas y restricciones para cualquier cambio referente al sistema operativo y sus configuraciones. c. Las computadoras deberán estar conectadas únicamente a las redes de datos de la organización, esto garantiza la protección al estar sujetas a las políticas, controles y restricciones definidas por los administradores de red. d. Todas las computadoras utilizadas en el Sistema de Botones de Seguridad, deberán estar sujetas a las políticas establecidas por la Unidad de Soporte Técnico del MDI, esto implica estar dentro de los dominios establecidos y mantener la protección del software antivirus corporativo.	

Elaborado por: autor de la Investigación

Tabla 19.- Seguridad en las Telecomunicaciones

INSTITUCIÓN	**MINISTERIO DEL INTERIOR – SISTEMA DE BOTONES DE SEGURIDAD**
POLÍTICA	**POLÍTICA DE SEGURIDAD EN LAS TELECOMUNICACIONES**
OBJETIVO	Asegurar la información en las redes y en los procesos de intercambio de información.

GESTIÓN EN LA SEGURIDAD DE LAS REDES	
Mecanismos de seguridad asociados a servicios de red	**Referencia: 13.1.2**

a. Todas las computadoras utilizadas en la Unidad Técnica Administrativa y Unidad de Coordinación de Policía Comunitaria, deberán estar asociadas únicamente a la red de datos institucional.
b. Todas las computadoras de la Unidad Operativa (UPC), deberán estar únicamente asociadas a la red de datos y servicios de las UPC a nivel nacional.
c. Las computadoras asociadas a la red institucional y a la red de datos y servicios de las UPC, estarán sujetas a las políticas y normativas definidas por la administración de redes e infraestructura tecnológica del Ministerio del Interior, lo cual incluye:
    - ✓ Filtrado de páginas no autorizadas
    - ✓ Filtrado de contenidos
    - ✓ Protección web
    - ✓ Protección en el correo electrónico
    - ✓ Protección de servidores web
    - ✓ Sistema de Detección de Intrusos
    - ✓ Sistema de Protección de Intrusos
    - ✓ Control y protección en los puertos de comunicación

INTERCAMBIO DE INFORMACIÓN CON PARTES EXTERNAS	
Acuerdos de intercambio	**Referencia: 13.2.2**

a. La organización o institución externa deberá remitir de manera formal y dirigida a la máxima autoridad del MDI, una solicitud en la que se especifique la información requerida y el propósito que se dará a la misma, aplicará a todos los datos almacenados en la base de datos del sistema de Botones de Seguridad.
b. Para el caso de requerimientos institucionales internos se aplicará el mismo procedimiento descrito en el literal anterior.
c. La máxima autoridad del MDI o su delegado, serán las únicas personas que autoricen y dispongan la entrega de la información.
d. La información a ser entregada independientemente del medio en el cual se almacene, deberá estar dentro de un sobre cerrado, etiquetado acorde a la nomenclatura de clasificación de la información institucional y con su sello de seguridad respectivo.
e. El documento o paquete a enviar deberá estar sometido a las políticas de mensajería institucional a través de los registros en el envío, transporte y entrega.
f. Las fallas en el manejo de envío, transporte y entrega estarán sometidas a las normativas vigentes institucionales, establecidas dentro de las Obligaciones y Responsabilidades en caso de pérdida de la información

Acuerdos de confidencialidad y secreto	**Referencia: 13.2.4**

a. El acuerdo de confidencialidad de la información a suscribirse, deberá contener en sus cláusulas los siguientes aspectos:
    - ✓ Comparecientes

- ✓ Antecedentes
- ✓ Definiciones
- ✓ Objeto
- ✓ Obligación reservada
- ✓ Sanciones o indemnizaciones
- ✓ Vigencia

b. Los Acuerdos de confidencialidad deberán ser suscritos en los siguientes casos:

- ✓ Entrega de información de la base de datos parcial o completa del Sistema de Botones de Seguridad tanto en requerimientos externos como internos
- ✓ Entrega de cuentas con privilegios y acceso total a la información
- ✓ Suscripción de contratos con proveedores de servicios que requieran acceso a la información de la base de datos

c. Para el caso de los acuerdos de confidencialidad de la información anexos a los contratos con proveedores, deberá solicitarse la elaboración y validación por parte de la Dirección Jurídica Institucional

Elaborado por: autor de la Investigación

Tabla 20.- Relaciones con los Suministradores

INSTITUCIÓN	**MINISTERIO DEL INTERIOR – SISTEMA DE BOTONES DE SEGURIDAD**
POLÍTICA	**POLÍTICA DE RELACIÓN CON LOS SUMINISTRADORES**
OBJETIVO	Asegurar la confidencialidad, integridad y disponibilidad de la información en los procesos de compra, arrendamiento y contratación de servicios con terceros.

SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON SUMINISTRADORES	
Tratamiento del riesgo dentro de acuerdos de suministradores	**Referencia:15.1.2**
a. La documentación como los contratos, términos de referencia, especificaciones técnicas, actas de entrega recepción y demás documentación que garantice la correcta administración, aseguramiento, obligaciones, costes, multas, plazos y otros aspectos de importancia a considerar en la relación entre el Ministerio del Interior a través de la Coordinación de TICs y los proveedores, deberán tener su sustento en Ley Orgánica del Sistema Nacional de Contratación Pública durante los procesos pre contractuales y contractuales. b. Para el servicio que brinda el alojamiento de los datos y registros del Sistema de Botones de Seguridad, es necesario suscribir un Acuerdo de Confidencialidad de la Información, este documento deberá garantizar la confidencialidad, integridad y disponibilidad de la información, así como establecer las posibles sanciones o multas a la que incurriera la empresa proveedora de servicio en caso de fallar a cualquier clausula establecida en el acuerdo.	
GESTIÓN DE LA PRESTACIÓN DEL SERVICIO POR SUMINISTRADORES	
Supervisión y revisión de los servicios prestados por terceros	**Referencia:15.2.1**
a. Acorde a lo establecido en la Ley Orgánica del Sistema Nacional de Contratación Pública; la máxima autoridad del MDI, designará un Administrador del Contrato, quien será el responsable de velar por el cumplimiento de los términos, acuerdos y especificaciones	

técnicas establecidas en los contratos y demás documentos suscritos con los proveedores de servicios tecnológicos, además de designar un técnico afín o fiscalizador de los contratos asociados a proyectos y servicios tecnológicos.

b. El o los funcionarios delegados, deberán monitorear los servicios tecnológicos, a fin de que se cumpla la "Disponibilidad mínima mensual" establecida en los SLA o Acuerdos de Nivel de Servicio, suscritos con los proveedores.
c. El o los funcionarios delegados, deberán revisar los informes mensuales de disponibilidad técnica remitidos por los proveedores de servicio; en caso de que un proveedor no cumpla con los niveles establecidos, deberán informar al Coordinador General de TICs además de considerar las multas o sanciones especificadas en los contratos.
d. Referente al servicio del Integrador SMS, se deberá establecer un procedimiento para comprobar que el número de SMS facturados, efectivamente corresponde a las alarmas generadas a través del Sistema de Botones de Seguridad.

Elaborado por: autor de la Investigación

Tabla 21.- Gestión de incidentes en la seguridad de la información

INSTITUCIÓN	**MINISTERIO DEL INTERIOR – SISTEMA DE BOTONES DE SEGURIDAD**
POLÍTICA	**POLÍTICA DE GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**
OBJETIVO	Asegurar un correcto y adecuado proceso en la comunicación y notificación de incidentes de seguridad de la información, así como la respuesta a estos en caso de presentarse.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS	
Notificación de los eventos de seguridad de la información	**Referencia: 16.1.2**

a. Es obligación de todos los funcionarios comunicar los eventos de seguridad de la información.
b. En caso de presentarse eventos de seguridad de la información, los funcionarios deberán notificar a través de un correo a la siguiente dirección: egsi@ministeriodelinterior.gob.ec
c. Se considerarán como eventos de seguridad las siguientes acciones:
    - ✓ Controles inadecuados de la seguridad
    - ✓ Errores humanos
    - ✓ No cumplir con las políticas o directrices establecidas por la institución
    - ✓ Fallas en el funcionamiento de software o hardware
    - ✓ Incumplimiento a las normativas establecidas en relación a la seguridad física
    - ✓ Violaciones de acceso
    - ✓ Violación o quebrantamiento de la confidencialidad, integridad o disponibilidad de la información

Respuesta a los incidentes de seguridad	**Referencia: 16.1.5**

a. Se deberá recolectar información que permita evidenciar el incidente ocurrido, así como identificar el origen del mismo.
b. Todas las actividades que se ejecuten como respuesta al incidente deberán ser registradas de manera correcta para los análisis posteriores.
c. El oficial de Seguridad de la información deberá mantener un registro de los incidentes de

seguridad notificados, esta acción servirá como retroalimentación para establecer correcciones y controles apropiados y oportunos

Elaborado por: autor de la Investigación

Tabla 22.- Seguridad de la información en la gestión de la continuidad del negocio

INSTITUCIÓN	**MINISTERIO DEL INTERIOR – SISTEMA DE BOTONES DE SEGURIDAD**
POLÍTICA	**POLÍTICA DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**
OBJETIVO	Asegurar la disponibilidad de la información a través de procesos que eviten caídas o pérdidas de información en los sistemas y servicios tecnológicos.
REDUNDANCIAS	
Disponibilidad de instalaciones para el procesamiento de información	**Referencia: 17.2.1**
a. Debido a la importancia y criticidad de los servicios que forman parte de la plataforma tecnológica del sistema de Botones de Seguridad, la Coordinación General de TICs deberá establecer en los Términos de Referencia y Especificaciones Técnicas que la empresa proveedora de servicios garantice la disponibilidad de los mismos a través de una solución basada en arquitecturas redundantes.	

Elaborado por: autor de la Investigación

Tabla 23.- Cumplimiento

INSTITUCIÓN	**MINISTERIO DEL INTERIOR – SISTEMA DE BOTONES DE SEGURIDAD**
POLÍTICA	**POLÍTICA DE CUMPLIMIENTO**
OBJETIVO	Evitar incumplimientos de las normas y directrices relacionadas a la seguridad de la información.
REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN	
Cumplimiento de las políticas y normas de seguridad	**Referencia: 18.2.2**

a. El Coordinador General de TICs tendrá la atribución de evaluar el cumplimiento de las normativas establecidas en el presente documento.
b. El Coordinador General de TICs deberá solicitar los entregables o documentos de respaldo que sustenten la gestión realizada en referencia a las normativas de seguridad establecidas; entre los principales entregables podrán considerarse:
    - ✓ Informe de repositorio de cuentas del sistema web de Botones de Seguridad
    - ✓ Informe de cuentas asignadas clasificadas según los perfiles de usuario
    - ✓ Informe de revocatoria o dada de baja de cuentas del sistema web de Botones de Seguridad
    - ✓ Informe de conformidad de servicios realizados por los Administradores de Contrato
    - ✓ Informe de servicios de los técnicos o fiscalizadores responsables de los contratos
    - ✓ Informe de disponibilidad de servicios y recursos tecnológicos asociados al

Sistema de Botones de Seguridad

- ✓ Informe del plan de mantenimiento ejecutado
- ✓ Informe de peticiones y entrega de información con sus respectivos acuerdos de confidencialidad en el caso que amerite
- ✓ Toda la documentación que se considere necesaria

c. Toda la documentación y procesos podrán estar sujetos a un proceso de auditoría interno o externo

d. Para los procesos de auditoría se deberá tomar como referencia la Norma 410, contemplada en las Normas de Control Interno de la Contraloría General del Estado.

e. Los Contratos suscritos con terceros, pueden estar sujetos a Exámenes Especiales establecidos por la Contraloría General del Estado; para lo cual se deberá tomar muy en cuenta las normativas establecidas por dicha entidad de control.

Elaborado por: autor de la Investigación

CONCLUSIONES

- ✓ Mediante el estándar para la gestión de la seguridad de la información descrito a través de la Norma ISO/IEC 27002:2013, fue posible diseñar la Política de Seguridad de la Información para el Sistema de Botones de Seguridad del Ministerio del Interior, la misma que está aplicada a los procesos de manejo de los servicios de la plataforma tecnológica y a los entornos o unidades administrativas de este sistema de seguridad integral, orientando a la correcta administración y gestión de la información.
- ✓ Existen amenazas y vulnerabilidades a las cuales están expuestos los activos del Sistema de Botones de Seguridad del Ministerio del Interior; esta afirmación es el resultado del levantamiento de información y de la matriz de riesgos, elaborada de acuerdo a la determinación de amenazas y vulnerabilidades, estimación del impacto y el riesgo sobre los activos; procedimiento que fue sustentado y elaborado de acuerdo a la Metodología MAGERIT.
- ✓ De acuerdo a la criticidad de los activos, tipo de información manejada y objetivos organizativos del Sistema de Botones de Seguridad como parte de la Coordinación General de TICs del Ministerio del Interior, se ha seleccionado un total de 25 controles, de la norma NTE INEN ISO/IEC 27002:2013, los mismos que son los más adecuados y que mejor se adaptan para minimizar el riesgo que pueda ocasionar la materialización de las amenazas sobre los activos.

- ✓ La Política de Seguridad de la Información propuesta, contiene los aspectos, características y buenas prácticas recomendadas para la gestión de la seguridad de la información de acuerdo a la norma NTE ISO/IEC 27002:2013, además de la definición y objeto, terminología, abreviaturas y responsabilidades; con la finalidad de que su aplicación y aprobación a través de la Coordinación General de TICs del Ministerio del Interior, requiera un mínimo de modificaciones.

RECOMENDACIONES

- ✓ De acuerdo a la experiencia adquirida en el presente trabajo, el aplicar la Metodología Magerit ha proporcionado una guía práctica y adecuada a la hora de abarcar el análisis y la gestión de los riesgos, en tal razón se puede recomendar esta la metodología para proyectos, planes y procesos que requieran una estructura sistemática y organizada para la gestión de riesgos.
- ✓ Con la finalidad de que la Política de Seguridad de la información cumpla con el objetivo planteado que es el garantizar la seguridad de la información dentro del Sistema de Botones de Seguridad y una vez implementada, es necesario realizar una evaluación periódica para verificar si los funcionarios cumplen con las normativas definidas y si los controles aplicados están realmente satisfaciendo las necesidades de seguridad para las cuales fueron escogidas.
- ✓ La Coordinación General de Tecnologías de la Información deberá liderar y promover capacitaciones sobre la importancia de la seguridad de la información en el Ministerio del Interior, así como asesorar a la alta dirección en el desarrollo planes, políticas o sistemas de seguridad de la información que precautelen la gestión y administración de la información, más aún si en esa Cartera de Estado se maneja información sensible y confidencial.

- ✓ En base a la Política de seguridad diseñada y con la finalidad de complementar normativas generales basadas en la Norma ISO/IEC 27002:2013, se sugiere como trabajo futuro, Diseñar un modelo de Política de Seguridad de la Información que pueda implementarse en los departamentos de Tecnologías de la Información en cualquier entidad del sector público, cuyo estatuto o nivel organizacional se encuentre a nivel de una Coordinación.

BIBLIOGRAFÍA

AGUILERA, P., 2010. *Seguridad Informática* [en línea]. S.l.: s.n. Disponible en: https://books.google.es/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=riesgos+en+los+sistemas+informaticos&ots=PqnsPzBET0&sig=u8aXGAiJYbf6L_bZeYlJXe6W_Ls#v=onepage&q&f=false.

AYRES SFREDDO, J. y FLORES, D., 2012. Segurança da informação arquivística: o controle de acesso em arquivos públicos estaduais. *Perspectivas em Ciência da Informação* [en línea], pp. 158-178. Disponible en: http://bit.ly/2zUJcnz.

CONTRERAS, L., 2016. *Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/iec 27001 para la dirección de sistemas de la gobernación de Boyacá*. [en línea]. S.l.: s.n. Disponible en: http://hdl.handle.net/10596/11895.

DSTU/MDI, 2018a. PERFIL DE PROYECTO BOTONES DE SEGURIDAD. . S.l.:

DSTU/MDI, 2018b. TÉRMINOS DE DE REFERENCIA PLATAFORMA BOTONES DE SEGURIDAD. . S.l.:

EGSI, 2013. Esquema Gubernamental de Seguridad de la Información.

EL COMERCIO, 2015. *Ecuador se muestra vulnerable a ciberataques | El Comercio* [en línea]. 2015. S.l.: 2015-07-26. [Consulta: 9 enero 2019]. Disponible en: https://www.elcomercio.com/actualidad/ecuador-muestra-vulnerable-ciberataques.html.

FERNÁNDEZ, G., 2018. El concepto de riesgo, probabilidad e impacto a la hora de realizar la evaluación de impacto de protección de datos. [en línea]. Disponible en: https://www.iberley.es/revista/concepto-riesgo-probabilidad-impacto-evaluacion-impacto-proteccion-datos-219.

GARAVITO, H., 2015. *Análisis y gestión del riesgo de la información en los sistemas de información misionales de una entidad del estado, enfocado en un sistema de seguridad de la información.* S.l.: UNIVERSIDAD ABIERTA Y A DISTANCIA ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA BOGOTÁ.

GÓMEZ, A., 2011. *Enciclopedia de la seguridad informática*. Vol. 6. S.l.: s.n.

GÓMEZ, S., 2007. Seguridad De La Información. *Universidad Nacional de Ingeniería* [en línea], pp. 500. ISSN 1815-0268. DOI 10.13128/ijae-9077. Disponible en: http://cybertesis.uni.edu.pe/handle/uni/9764%0Ahttp://cybertesis.uni.edu.pe/bitstream/uni/9764/1/gomez_fs.pdf.

HALLBERG, J. y HUNSTAD, A., 2005. A frmewor for system security assessment. *Information Assurance Workshop*, vol. Six annual, pp. 25.

INFOBAE, 2011. *No Title* [en línea]. 2011. S.l.: 2011-08-09. Disponible en: http://www.seguridadydefensa.com.ec/noticias/anonymus-revelo-datos-de-45-mil-policias-24513.html.

INTERIOR, M. del, 2012. No Title. [en línea]. Disponible en: https://www.brandsoftheworld.com/logo/ministerio-del-interior.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2017. When the world agrees. [en línea]. Disponible en: https://www.iso.org/standard/54533.html.

ISO, 27001. *Norma Técnica Ecuatoriana*. 27001. S.l.: s.n.

ISO TOOLS EXCELLENCE, 2016. La norma ISO 27002 complemento para la ISO 27001. [en línea]. [Consulta: 20 enero 2019]. Disponible en: https://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/.

LADINO, M.I. y VILLA, P.A., 2014. Fundamentos de ISO 27002 y su aplicacion en las empresas. *Scientia et Technica* [en línea], vol. 334. Disponible en: http://www.redalyc.org/html/849/84921327061/.

LEDEZMA, D., 2015. *Desarrollo de políticas de seguridad de la Información basadas en las normas ISO 27002 para una Coordinación zonal del INEC* [en línea]. S.l.: Pontificia Universidad Católica del Ecuador Sede Ambato. Disponible en: http://repositorio.pucesa.edu.ec/handle/123456789/1555.

MENDEZ, A., MESA, J., ZAPICO, F. y GUERREO, V., 2003. Techno-Legal Aspects of Information Society and New Economy: an Overview. [en línea], pp. 187. Disponible en: http://mario.elinos.org.mx/publication/papers/2003/002.pdf.

MENTOR, 2016. Normas ISO sobre gestión de seguridad de la información | Seguridad Informática. [en línea]. Disponible en: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS., 2012. *Metodología de*

Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I. S.l.: Version 3.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, 2012. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Libro III. S.l.: s.n.

RECIO, M.J., 2012. De la Seguridad Informática a la Seguridad de la Información. *Artículo Seguridad y Salud* [en línea], pp. 14-19. Disponible en: https://www.aec.es/c/document_library/get_file?uuid=e25028ca-cb3b-4ffd-ada0-4ce2efa86f80&groupId=10128.

RODRÍGUEZ, A., 2016. *La importancia de la Seguridad Informática - Trustdimension* [en línea]. 2016. S.l.: s.n. [Consulta: 9 enero 2019]. Disponible en: https://www.trustdimension.com/la-importancia-de-la-seguridad-informatica/.

TÉLLEZ, J., 2014. *Contratos, riesgos y seguros informáticos*. México DF: Universidad Autónoma de México.

ANEXO 1: Autorización Ministerio del Interior

GOBIERNO NACIONAL DE LA REPÚBLICA DEL ECUADOR

Ministerio del Interior

Benalcázar N4-24 entre Espejo y Chile
PBX 593-2 295-5666 295-0470
www.ministeriodelinterior.gob.ec

Memorando Nro. MDI-CGTI-2018-055-E
Quito, D.M., 14 de mayo de 2018

PARA: Sr. Ing. Marcelo Contero

De mi consideración:

Con un atento y cordial saludo, en base al oficio Nro. MC-2018-0012 del 8 de mayo de 2018, mediante el cual se solicita la autorización para poder realizar el trabajo de investigación Diseño de una Política De Seguridad De La Información Basada En La Norma ISO 27001 Y 27002, para el Sistema De Botones de Seguridad Del Ministerio Del Interior; tengo a bien indicar que su requerimiento ha sido autorizado.

En base a lo anteriormente indicado, solicito de la manera más comedida todos los trabajos que requiera levantamiento y acciones correspondientes sean debidamente coordinados a través de la Dirección de Soporte Técnico a Usuarios; así como también agradecería se presente un informe de los resultados obtenidos a fin de analizar la factibilidad de implementación dentro de esta institución.

Finalmente, pongo a su disposición las facilidades necesarias para una exitosa culminación de sus objetivos, así como también solicito la discrecionalidad de la información.

Con sentimientos de distinguida consideración.

Atentamente,

COORDINACIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Ministerio del Interior

Ing. Pablo Renato Escobar Vallejos
COORDINADOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Copia: Sra. Mgs. Alejandra Isabel Alvarez Cedeño
Directora de Soporte Técnico a Usuarios

ANEXO 2: controles norma NTE INEN ISO/IEC 27002:2013

Quito – Ecuador

NORMA
TÉCNICA
ECUATORIANA

NTE INEN-ISO/IEC 27002
Segunda edición

TECNOLOGÍAS DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – CÓDIGO DE PRÁCTICA PARA LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN (ISO/IEC 27002:2013+Cor. 1:2014+Cor. 2: 2015, IDT)

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS (ISO/IEC 27002:2013+Cor.1:2014+Cor.2:2015)

Correspondencia:

Esta Norma Técnica Ecuatoriana es una traducción idéntica de la Norma Internacional ISO/IEC 27002:2013+Cor.1:2014+Cor.2:2015.

ICS: 35.040

94
Páginas

CON LICENCIA DE USO PARA MARCELO CONTERO RAMOS, POR INEN
NÚMERO DE ORDEN: 001 - 005 - 000109109/ DESCARGADO: 2019-01-29
AUTORIZACIÓN A USUARIO ÚNICO, PROHIBIDA SU REPRODUCCIÓN

© ISO/IEC 2015 – Todos los derechos reservados
© INEN 2017

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

ISO/IEC 27002:2013

ISO27002.es PATROCINADO POR:

GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

Iso27000.es: Documento sólo para uso didáctico. La norma oficial debe adquirirse en las entidades autorizadas para su venta.

Octubre-2013

ANEXO 3: Formato de la propuesta de la Política de Seguridad

MINISTERIO DEL INTERIOR

COORDINACIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN

SISTEMA DE BOTONES DE SEGURIDAD

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

REFRENCIA: NTE INEN-ISO/IEC 27002:2013

VERSIÓN 1.0

FEBRERO DEL 2018

FIRMAS DE REVISIÓN Y APROBACIÓN

Registro Del Documento			
Acción	**Nombre / Cargo**	**Firma**	**Fecha**
Elaborado por:	Ing. Marcelo Contero Ramos / Estudiante MTI – UISEK		Febrero de 2019
Revisador por:	Ing. María Verónica Loarte / Oficial de Seguridad de la Información Msc. Alejandra Alvarez / Directora de Soporte Técnico a Usuarios		
Aprobador por:	Ing. Pablo Escobar Vallejos / Coordinador General de TICs		
Revisión Técnica	Ing. Gabriela Calero / Líder Metodológico de Procesos		

CONTROL E HISTORIAL DE CAMBIOS

Versión	Descripción del cambio	Fecha de actualización
1.0		