TRABAJO FINAL DE MASTER.

# DESARROLLO DE UN PLAN DIRECTOR DE SEGURIDAD DE INFORMACIÓN PARA LA EMPRESA “AGUAS DE MANTA”.

**Nombre Estudiante:** Italo Hernández Valencia

**Programa:** Máster Interuniversitario en Seguridad de las TICS (MISTIC).

**Área:** Sistemas de Gestión de la Seguridad de la Información

**Consultor:**
**Profesor responsable de la asignatura:** Carles Garrigues Olivella

**Centro:** Universitat Oberta de Catalunya

**AUTOR:** ITALO HERNÁNDEZ V.

- **FICHA DEL TRABAJO FINAL**

| | |
|---|---|
| **Título del trabajo:** | *Trabajo final de máster.* |
| **Nombre del autor:** | *Italo Hernández Valencia* |
| **Nombre del consultor/a:** | *Antonio Segovia Henares* |
| **Nombre del PRA:** | *Carles Garrigues Olivella* |
| **Fecha de entrega (mm/aaaa):** | 05/2021 |
| **Titulación:** | Máster Interuniversitario en Seguridad de las TICS (MISTIC) |
| **Área del Trabajo Final:** | *Sistemas de Gestión de la Seguridad de la Información* |
| **Idioma del trabajo:** | *Español - Castellano* |
| **Palabras clave** | *Análisis , Metodología, Seguridad, Información, Sistema , Gestión , Riesgos.* |


**Resumen del Trabajo (máximo 250 palabras):**

*Este documento tiene como finalidad principal proveer una guía metodológica que oriente al personal encargado de la gestión de la seguridad de la información de la Empresa Pública Aguas de Manta, conforme al despliegue completo de los procedimientos que debe seguir la organización con miras a establecer una gestión controlada y efectiva respecto a seguridad de Información.*

*Su contexto encierra todo lo concerniente a la implantación de un modelo de gestión basado en las mejoras prácticas y controles anexos a la norma ISO 27001/IEC:2013 , en conjunto con la metodología de Análisis de Riesgos Magerit Versión 3.0*

*En síntesis este plan constituye la hoja de ruta que debe seguir la empresa para establecer controles, alcanzar metas y cumplir con indicadores que permitan conocer el estado de esta respecto a seguridad de la información, sin restarle importancia al despliegue de acciones que se deben ejecutar para mejorarla.*

*Los resultados están a la vista, el análisis de riesgos y los proyectos propuestos en los siguientes capítulos son contundentes respecto a que la desatención de la seguridad de información desemboca en costosas consecuencias económicas y operativas para la organización.*

**Abstract (in English, 250 words or less):**

The main purpose of this document is to provide a methodological guide, to the personnel in charge of managing the information security of the "Aguas de Manta" Public Company, in accordance with the complete deployment of the procedures that the organization must follow in order to establish a management controlled and effective regarding information security.

Its context encompasses everything concerning the implementation of a management model based on the best practices and controls annexed to the ISO 27001 / IEC: 2013 standard, in conjunction with the Magerit Version 3 Risk Analysis methodology.

In summary, this plan constitutes the roadmap that the company must follow to establish controls, achieve goals and comply with indicators that allow knowing the state of this with respect to information security, without diminishing the importance of the deployment of actions that must be carried out to improve it.

The results are in sight, the risk analysis and the projects proposed in the following chapters are conclusive regarding the fact that the neglect of information security leads to costly economic and operational consequences for the organization.

**DEDICATORIA**

Dedico el esfuerzo y la dedicación que entregué en la realización de este trabajo final de Máster a mis hijos Emiliano y Alina, a mi esposa y amiga Evelyn, quien me brindó el apoyo y la confianza que me permitieron alcanzar mis metas. A mis padres Italo y Patricia, por siempre ofrecerme su apoyo y el empuje que necesitaba para continuar con mis estudios. A mis hermanos Angelo, Emily e Imannol. A mis abuelos Peter y Carmen por su orientación y paciencia. A todos mis familiares y amistades que en su momento me apoyaron con sus mejores deseos.

Dedico este trabajo a quienes comenzaron conmigo este proceso, el cual demandó mucho esfuerzo y sacrificio, factores q sobrellevamos a través de las circunstancias, asimismo dedico el presente trabajo para que sirva de estímulo a quienes quieran incursionar en este largo camino de formación académica.

Para aquellos profesionales que me sirvieron de inspiración para terminar esta etapa de adquisición de conocimiento que realmente cambia y transforma a la persona. Y a todos los que se esfuerzan día a día para generar pasos de bienestar para los demás.

**AGRADECIMIENTO**

Mi agradecimiento a Dios, por ser mi sustento principal en este largo proceso de aprendizaje, reconociendo que sin su bendición no hubiera podido culminarlo.

Agradezco también a la UOC por el conocimiento brindado mediante sus excelentes docentes, quienes siempre demostraron profesionalismo y compromiso.

A Antonio Segovia, tutor del presente trabajo final de máster por su valiosa contribución y guía en el desarrollo del proyecto.

Y finalmente a mi esposa, amiga y compañera Evelyn Cano quien fue la precursora de que retomé mis estudios y me apoyó absolutamente en cada uno de los pasos que emprendí y seguiré emprendiendo.

**AUTOR:** ITALO HERNÁNDEZ V.

# Índice

Contenido

# Tabla de ilustraciones.



# Índice de tablas.

# 1. Objetivos y análisis diferencial.

## 1.1 Introducción

Partiendo de la premisa universal de que la información se ha convertido en un activo transcendental para la operatividad de una organización y por ende es de suma importancia protegerla, podemos declarar de manera segura que la Seguridad de la información es el conjunto de técnicas, normativas y requisitos que encierran todo lo relacionado con la protección de la información independiente de su naturaleza (digital, documental, etc.), se refiere principalmente a asegurar la integridad, confidencialidad y disponibilidad de los datos de una organización.

El plan director de seguridad es sin duda una herramienta indispensable para el responsable de la Seguridad de la información en una entidad, ya que mediante este insumo se realizará el despliegue completo acerca de los procedimientos que debe seguir la organización con miras a establecer una gestión controlada y efectiva respecto a este rubro.

En síntesis este plan constituye la hoja de ruta que debe seguir la empresa para establecer controles, alcanzar metas y cumplir con indicadores que permitan conocer el estado de esta respecto a seguridad de la información, sin restarle importancia al despliegue de acciones que se deben ejecutar para mejorarla, sin olvidar que estamos hablando por tanto de un modelo de mejora continua PDCA (Plan-Do-Check-Act).

El marco legal ha reflejado la importancia de la seguridad de la información, en el Ecuador bajo la secretaría de gobierno electrónico mediante el Esquema Gubernamental de Seguridad de la Información (EGSI) y a nivel legislativo bajo el Código Orgánico Integral Penal. En el país La seguridad de la información se ha posicionado de manera protagónica y queda claro que no se trata de un aspecto opcional, sino que debe ser inherente a las actividades de la propia empresa, y constituye un punto de partida ineludible en lo que a gestión organizacional se refiere.

Como insumo final el plan director tiene como primicia sentar las bases de un esquema de Seguridad para la empresa. Empezando por tareas simples pero efectivas, a continuación, detallamos un breve extracto de las principales actividades a realizar.

- Analizar y detallar nuestro inventario de activos.
- Estudiar las amenazas a las que están expuestos.
- Estudiar el impacto potencial de dichas amenazas.
- Proponer un plan de acción para luchar contra dichas amenazas.
- Evaluar el impacto residual una vez aplicado el plan de acción.

Los aspectos no contemplados en el listado anterior tienen que ver con la operatividad y la organización que tácitamente vienen de la mano con las actividades mencionadas, sin embargo las iremos abordando poco a poco durante el despliegue de tareas en nuestro proyecto.

## 1.2 Conociendo La ISO/IEC 27002:2013

Es necesario mencionar que la evolución y el protagonismo que ha ganado la seguridad de la información esto le ha ayudado a posicionarse como una medida obligatoria en todo lo concerniente a sistemas de información. Así de esta misma manera las metodologías y las

buenas prácticas han ganado su espacio al momento de buscar alternativas y estrategias sobre seguridad de la información.

Por ello, hemos creído relevante disponer de una primera etapa donde nos documentaremos de algunas de las mejores prácticas en seguridad de la información. Estas 'mejores prácticas' serán fundamentales para realizar una aproximación sistemática al análisis de la seguridad. Aun cuando son muchas las aproximaciones, nosotros nos centraremos en el estudio de la ISO/IEC 27001. Es por ello, que en esta fase, nos documentaremos sobre la misma y compartiremos las impresiones o dudas que puedan generarse al respecto. Remarcar antes de su lectura que se trata de un documento de buenas prácticas concretadas mediante un conjunto de controles.

La **ISO 27001** es un estándar internacional regentado por la Organización Internacional de Normalización (ISO) , y detalla la gestión de la seguridad de la información en una empresa. La última revisión oficial fue publicada en 2013 y renombrada como: ISO/IEC 27001:2013.

Esta norma goza de basto reconocimiento internacional y está redactada por los expertos certificados en el tema, este estándar proporciona una metodología de implementación y aplicabilidad que conlleva a la certificación, esto significa que es una norma idónea para que una entidad de certificación independiente declare que la gestión de seguridad de la información cumple con la norma ISO 27001. El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Tiene como premisa realizar hallazgos que evidencien problemas que podrían afectar la información y luego definiendo acciones para evitar que estos problemas se produzcan lo que al final será la mitigación o tratamiento del riesgo

Los controles se presentan por lo general, bajo la forma de políticas, procedimientos soluciones documentadas o técnicas ya que la gestión de la seguridad de la información no se encuentra limitada solamente a la seguridad de la infraestructura tecnológica sino que es necesaria la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

La filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, partiendo del principio que cada incidente, sea cual sea su naturaleza representa pérdidas económicas y evitándolos se supone un ahorro considerable en temas operativos y del flujo del negocio.

Ahora la **ISO 27002** reúne todos los controles que buscan mitigar el impacto o la posibilidad de ocurrencia de los diferentes riesgos a los cuales se encuentra expuesta la organización. Con la actualización de esta norma las organizaciones cuentan con una guía de implementación que sirve para la implementación de los controles de seguridad de la organización y de las prácticas más eficaces para gestionarla. Aun cuando son muchas las aproximaciones, nosotros nos centraremos en el estudio de la ISO/IEC 27002 (que proviene de la ISO 17799). Es por ello, que en esta fase, nos documentaremos sobre la misma y compartiremos las impresiones o dudas que puedan generarse al respecto. Remarcar antes de su lectura que se trata de un documento de 'buenas prácticas' concretadas mediante un conjunto de controles.

Además, cabe resaltar que existen versiones específicas de la norma ISO/IEC 27002, enfocadas en diferentes tipos de empresas: manufactureras, sector de la salud, sector financiero, entre otros. Si bien la nomenclatura ISO es diferente, son normas tienen como referencia el mismo estándar con el que estamos manejando el plan director actual.

## 1.3 Contextualización Y Alcance.

La empresa objeto de nuestro estudio es la Empresa Pública de Agua potable de Manta, una entidad gubernamental regida por la administración municipal que tiene como misión principal proveer servicios hidrosanitarios de producción y distribución de agua potable; recolección, tratamiento y disposición de aguas servidas y pluviales. La empresa visualiza proyectarse como un referente de impulso al desarrollo estratégico de la región con la prestación de servicios hidrosanitarios sostenibles, basados en responsabilidad social, cuidado de recursos, fuentes y competitividad.

El organigrama de la institución se divide en gerencias agregadores de valor, de asesoría y de apoyo. A continuación, visualizamos el organigrama estructural de la institución.

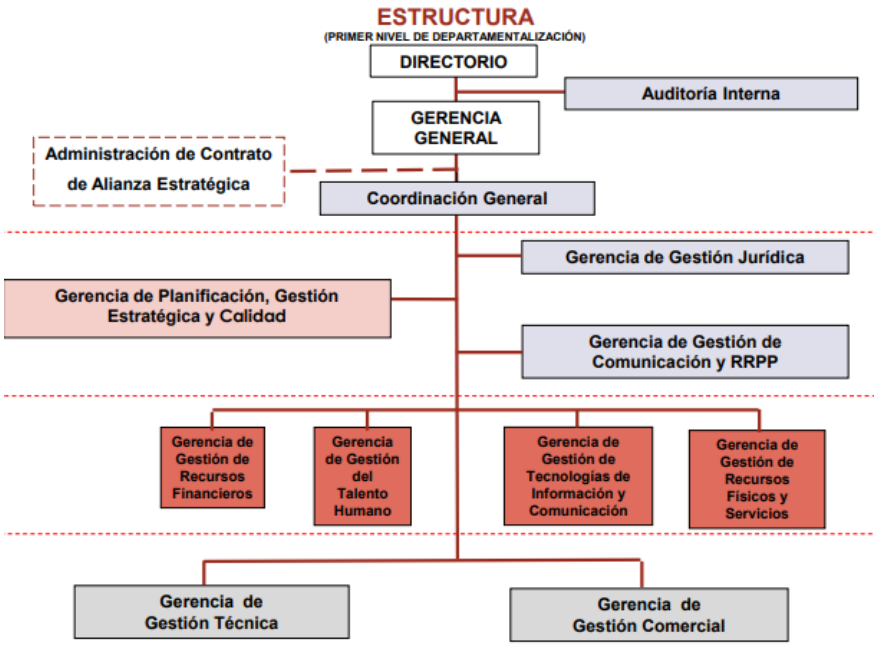
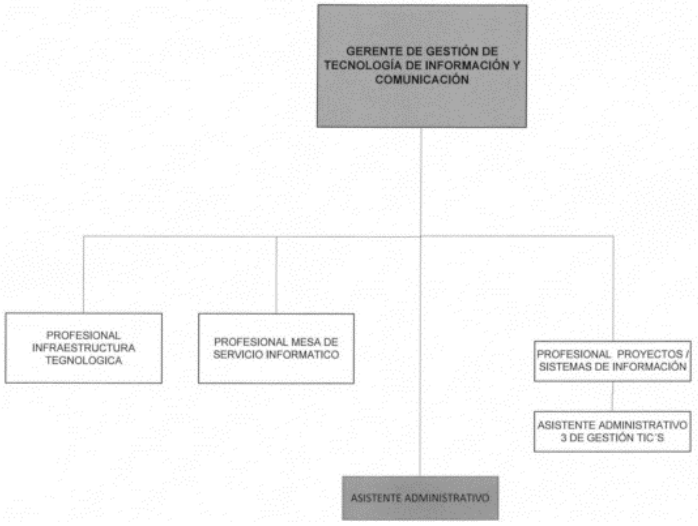



*Ilustración 1 - Organigrama EP Aguas de Manta*

La gerencia de TI como dirección habilitante de apoyo es responsable de brindar todos los servicios informáticos a los funcionarios, así mismo administra los recursos tecnológicos institucionales, genera e implementa la normativa relacionada, para garantizar la seguridad de la información digital y de los recursos tecnológicos que administra. En su estructura no cuenta con un profesional de Seguridad de Información.




La empresa tiene 7 estaciones, que se dividen en 3 plantas de tratamiento, 2 de aguas servidas , una estación de bombeo y una de aguas lluvias. Solamente 4 de estas estaciones cuentan con enlaces para la red de datos, en el siguiente esquema podemos conocer en detalle el esquema de conexión de las estaciones con la matriz.

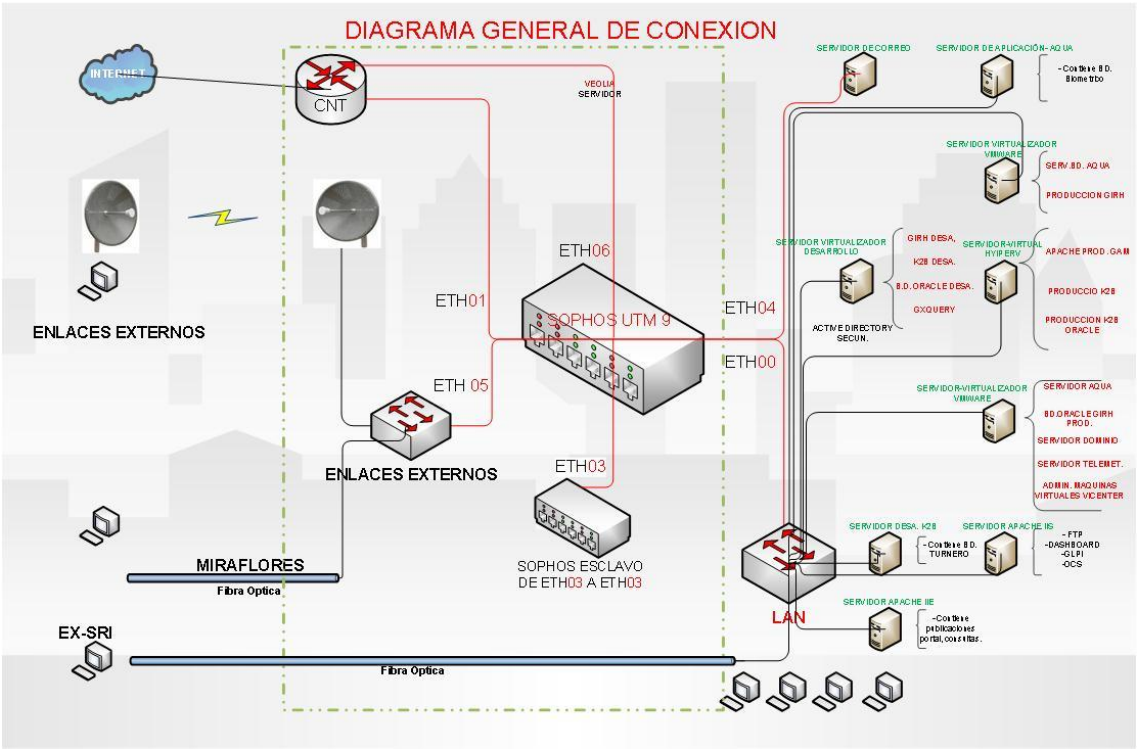



*Ilustración 3 - Diagrama de Red EP Aguas de Manta*

Como alcance establecemos que: el plan director a desplegar pretende normalizar la protección de toda la información física o digital, recibida o generada durante los procesos gobernantes, habilitadores de asesoría, habilitadores de apoyo y cadena de valor que realiza la entidad, así como la información que se encuentra bajo custodia de los empleados de la institución durante su proceso de atención de trámites y en archivos físicos, temporales o permanentes, bases de datos, almacenada en recursos tecnológicos a nivel de usuario y equipos servidores; de la misma manera se encuentra bajo esta tutela, junto con la información que se encuentra en etapa de

gestión de procesos internos. Es necesario implantar lineamientos anexos a procedimientos que orillen a los empleados en el cuidado y protección de la información institucional, que garantice a la empresa y a la ciudadanía en general la confidencialidad, integridad y disponibilidad de dicha información.

De igual manera es preciso establecer responsabilidades en torno a la organización la cual es responsable de la protección y custodia de la información recibida o generada por el personal interno y/o externo autorizado en la utilización de los distintos sistemas administrativos, aplicaciones informáticas y/o servicios tecnológicos asignados para el cumplimiento de sus funciones, atención de trámites y transacciones asociadas a su gestión; la misma podrá estar contenida en documentos, informes, reportes, bases de datos, archivos temporales o permanentes sean estos físicos o digitales, los cuales son sujeto de custodia y control de la empresa.

*Matriz DAFO para análisis estratégico*

| FACTORES INTERNOS DE LA EMPRESA | FACTORES EXTERNOS A LA EMPRESA |
|---|---|

| | DEBILIDADES (-) |
|---|---|
| 1 | Poca conciencia acerca de seguridad de información. |
| 2 | Informalidad en los procesos administrativos. |
| 3 | Prevalece la operatividad sobre la mejora continua. |
| 4 | Incorrecta gestión sobre activos tecnológicos. |
| 5 | Inexistencia de normativa y políticas sobre SI. |
| 6 | Burocracia excesiva e innecesaria. |
| 7 | Incidencia de terceros sobre procesos institucionales. |
| 8 | Excesivo uso de dispositivos personales. |
| 9 | Resistencia al cambio por parte de los empleados. |
| 10 | |

| | AMENAZAS (-) |
|---|---|
| 1 | Posee servicios tecnológicos publicados a la ciudadanía. |
| 2 | Infraestructura expuesta a amenazas. |
| 3 | No cuenta con plan de contingencia ante desastres. |
| 4 | Cambio de autoridades frecuentemente. |
| 5 | |
| 6 | |
| 7 | |
| 8 | |
| 9 | |
| 10 | |

| | FORTALEZAS (+) |
|---|---|
| 1 | Apoyo de autoridades actuales para implementar SGSI |
| 2 | Cuenta con personal profesional en Seg de Información. |
| 3 | Presupuesto asignado para mejoras tecnológicas. |
| 4 | Posee centro de datos con todos los estándares. |
| 5 | Posee infraestructura tecnológica moderna. |
| 6 | |
| 7 | |

| | OPORTUNIDADES (+) |
|---|---|
| 1 | Obligatoriedad de implementar EGSI. |
| 2 | Visión de implementar infraestructura cloud. |
| 3 | Tercerización se servicios tecnológicos. |
| 4 | Visión por certificarse en normas de calidad. |
| 5 | |
| 6 | |
| 7 | |

*Tabla 1 - Análisis DAFO.*

## 1.4 Objetivos Del Plan Director

Una vez conocida la normativa a aplicar, identificada la empresa y concretado el alcance es necesario establecer los objetivos del Plan Director de Seguridad.

Los principales objetivos del plan director a implementar son:

- **Garantizar la confidencialidad, integridad y disponibilidad de la información física y digital; gestión que a su vez debe estar alineada al cumplimiento de los objetivos institucionales.**
- Establecer normas y controles en la gestión de la seguridad de la información institucional.
- Mejorar de manera proactiva la gestión informática en los procesos que agregan valor a la EP Aguas de Manta.
- Asegurar la continuidad de las operaciones en torno a los sistemas de información críticos.
- Brindar un esquema que permita proteger la información institucional durante todo su ciclo de vida.
- Proveer capacitación continua para el talento humano de la organización en torno a temas de seguridad de la información.
- Adquirir capacidad de respuesta inmediata para atender incidentes de seguridad que puedan afectar el flujo de negocio de la organización.
- Implantar controles adecuados para el análisis y tratamiento de riesgos.
- Instaurar un esquema de buenas prácticas que apoye a la gestión del cambio en torno a la seguridad de la información corporativa.
- Establecer niveles de sensibilidad para la información y de respuestas a incidentes.
- Proteger la información mediante la implementación de medidas de seguridad preventivas, detectoras, de respuesta, y de recuperación.

## 1.5 Análisis Diferencial

Antes de iniciar el proyecto de implantación, tendremos que realizar un análisis diferencial de las medidas de seguridad y la normativa que tenga la Organización en relación con la Seguridad de la Información. Este análisis diferencial se realizará con respecto la ISO/IEC 27001:2013 e ISO/IEC 27002:2013, y nos permitirá conocer de manera global el estado actual de la Organización en relación de la Seguridad de la Información.

1. Respecto al análisis de requerimientos de la ISO/IEC 27001 :2013, capítulos del 4 al 10 realizamos el análisis mediante el siguiente esquema. El estado en el que se encuentra cada control se puede analizar en función del porcentaje: 0% ➔No aplicado. Del 10% - 50% ➔Fase inicial. Del 50% - 90 % ➔Fase intermedia, y si cuenta con el 100% ➔Completamente implementado.

| Análisis Diferencial respecto a la norma ISO 27001 | | % |
|---|---|---|
| Clausula 4 | Contexto de la organización | 13% |
| 4.1 | Entender la organización y su contexto | 30% |
| 4.2 | Entender las necesidades y expectativas de las partes interesadas | 10% |
| 4.3 | Determinar el alcance del SGSI | 0% |
| Clausula 5 | Liderazgo | 7% |
| 5.1 | Liderazgo y compromiso | 20% |
| 5.2 | Política | 0% |
| 5.3 | Roles de la organización, responsabilidades y autoridad | 0% |
| Clausula 6 | Planificación | 0% |

| | | |
|---|---|---|
| 6.1 | Acciones para dirigir los riesgos y oportunidades | 0% |
| 6.2 | Objetivos y planes para lograrlos | 0% |
| Clausula 7 | Soporte | 0% |
| 7.1 | Recursos | 0% |
| 7.2 | Competencias | 0% |
| 7.3 | Concienciación | 0% |
| 7.4 | Comunicación | 0% |
| 7.5 | Documentación | 0% |
| Clausula 8 | Operación | 10% |
| 8.1 | Planificación operativa y control | 10% |
| 8.2 | Análisis del riesgo | 10% |
| 8.3 | Tratamiento del riesgo | 10% |
| Clausula 9 | Evaluación del rendimiento | 0% |
| 9.1 | Monitorización, medición, análisis y evaluación | 0% |
| 9.2 | Auditoría interna | 0% |
| 9.3 | Revisión por Dirección | 0% |
| Clausula 10 | Mejora | 0% |
| 10.1 | No conformidad y acción correctiva | 0% |
| 10.2 | Mejora continua | 0% |

*Tabla 2 - Análisis Diferencial ISO27001.*

Respecto al análisis de controles del Anexo A de la ISO/IEC 27002:2013 , proponemos el siguiente GAP.

1

| CONTROL | | | Estado Actual | Estado de la organización |
|---|---|---|---|---|
| A.5 Information security policies | | | | |
| A.5.1 Management direction for information security | | | | |
| | A.5.1.1 | Policies for information security | 1 - Inicial | Existen políticas de seguridad de la información muy globales, y no se encuentran oficializadas ni difundidas . |
| | A.5.1.2 | Review of the policies for information security | 1 - Inicial | Existen políticas de seguridad de la información muy globales, y no se encuentran oficializadas ni difundidas . |
| A.6 Organization of information security | | | | |
| A.6.1 Internal organization | | | | |
| | A.6.1.1 | Information security roles and responsibilities | 1 - Inicial | La empresa acoge un procedimiento intuitivo pero que no se encuentra documentado, no hay roles ni responsabilidades definidas respecto a la gestión de la seguridad de la información. |
| | A.6.1.2 | Segregation of duties | 1 - Inicial | |
| | A.6.1.3 | Contact with authorities | 0 - No existente | No existe un procedimiento documentado acerca del contacto con las autoridades pertinentes ni organismos de control. |
| | A.6.1.4 | Contact with special interest groups | 0 - No existente | No existe un procedimiento documentado acerca del contacto con los grupos de interés. |
| | A.6.1.5 | Information security in project management | 0 - No existente | La gestión de proyectos sigue un flujo que no considera las repercusiones de no contar con seguridad de la información. |
| A.6.2 Mobile devices and teleworking | | | | |
| | A.6.2.1 | Mobile device policy | 1 - Inicial | Existen políticas segregadas basándose en buenas prácticas pero no se encuentran documentadas. |
| | A.6.2.2 | Teleworking | 1 - Inicial | La organización ha adoptado el Teletrabajo como una alternativa pero no existen normas ni procedimientos documentados sobre su correcto uso y el tratamiento de la información. |
| A.7 Human resource security | | | | |
| A.7.1 Prior to employment | | | | |
| | A.7.1.1 | Screening | 1 - Inicial | La organización solicita como requisito previo a la contratación el récord policial del postulante. |
| | A.7.1.2 | Terms and conditions of employment | 0 - No existente | No existe un procedimiento documentado acerca de socialización de políticas, términos y condiciones. |
| A.7.2 During employment | | | | |
| | A.7.2.1 | Management responsibilities | 1 - Inicial | |

| | | | |
|---|---|---|---|
| A.7.2.2 | Information security awareness, education, and training | 1 - Inicial | No existe un procedimiento documentado acerca de socialización de políticas , aunque se puede asumir el conocimiento tácito de las implicaciones que por ley corresponden. |
| A.7.2.3 | Disciplinary process | 1 - Inicial | |
| A.7.3 Termination and change of employment | | | |
| A.7.3.1 | Termination or change of employment responsibilities | 0 - No existente | No existe un procedimiento documentado de desvinculación que implique el respaldo de datos y seguridad de la información. |
| A.8 Asset management | | | |
| A.8.1 Responsibility for asset | | | |
| A.8.1.1 | Inventory of assets | 1 - Inicial | La empresa acoge un procedimiento intuitivo pero que no se encuentra documentado |
| A.8.1.2 | Ownership of assets | 1 - Inicial | La empresa acoge un procedimiento intuitivo pero que no se encuentra documentado |
| A.8.1.3 | Acceptable use of assets | 1 - Inicial | La empresa acoge un procedimiento intuitivo pero que no se encuentra documentado |
| A.8.1.4 | Return of assets | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante, el control no es previo , ni continuo, es posterior con muchas brechas de error. |
| A.8.2 Information classification | | | |
| A.8.2.1 | Classification of information | 2 - Repetible | Esta clasificación se encuentra en el borrador de la política de seguridad, la cual no se encuentra oficializada ni difundida. |
| A.8.2.2 | Labelling of Information | 2 - Repetible | |
| A.8.2.3 | Handling of assets | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante |
| A.8.3 Media handling | | | |
| A.8.3.1 | Management of removable media | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| A.8.3.2 | Disposal of media | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| A.8.3.3 | Physical media transfer | 0 - No existente | No existen herramientas ni procedimientos que normen este control. |
| A.9 Access control | | | |
| A.9.1 Business requirements of access control | | | |
| A.9.1.1 | Access control policy | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| A.9.1.2 | Access to networks and network services | 3 - Definido | El control de acceso a redes se encuentra normado por un sistema de seguridad perimetral , firewall y filtros de navegación. |
| A.9.2 User access management | | | |
| A.9.2.1 | User registration and de-registration | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante en todos los sistemas del catálogo de servicios. |

| | | | | |
|---|---|---|---|---|
| | A.9.2.2 | User access provisioning | 1 - Inicial | Los perfiles de usuarios y privilegios se encuentran definidos pero no son aplicables a los usuarios según la naturaleza de sus funciones. |
| | A.9.2.3 | Management of privileged access rights | 1 - Inicial | Los perfiles con accesos especiales no cuentan con un procedimiento documentado ni directivas establecidas correspondientes (complejidad , robustez , caducidad de contraseñas , umbral de intentos, etc.) |
| | A.9.2.4 | Management of secret authentication information of users | 0 - No existente | Los usuarios comparten contraseñas de las estaciones de trabajo, las claves de acceso a los sistemas regularmente son guardadas en el navegador. |
| | A.9.2.5 | Review of user access rights | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante ni bajo un cronograma establecido. |
| | A.9.2.6 | Removal or adjustment of access rights | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante ni bajo un cronograma establecido. |
| A.9.3 User responsibilities | | | | |
| | A.9.3.1 | Use of secret authentication information | 0 - No existente | No existen controles ni procedimientos que normen este apartado. |
| A.9.4 System and application access control | | | | |
| | A.9.4.1 | Information access restriction | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| | A.9.4.2 | Secure log-on procedures | 2 - Repetible | Existe la percepción de la existencia del control pero no se aplica de manera constante ni bajo un procedimiento establecido. |
| | A.9.4.3 | Password management system | 0 - No existente | No existen herramientas ni procedimientos que normen este control. |
| | A.9.4.4 | Use of privileged utility programs | 2 - Repetible | Existen políticas segregadas basándose en buenas prácticas pero no se encuentran documentadas. |
| | A.9.4.5 | Access control to program source code | 0 - No existente | No existen herramientas ni procedimientos que normen este control. |
| A.10 Cryptography | | | | |
| A.10.1 Cryptographic controls | | | | |
| | A.10.1.1 | Policy on the use of cryptographic controls | 5 - Optimizado | No existen herramientas ni procedimientos que normen este control. |
| | A.10.1.2 | Key management | 5 - Optimizado | No existen herramientas ni procedimientos que normen este control. |
| A.11 Physical and environmental security | | | | |
| A.11.1 Secure areas | | | | |

| | | | |
|---|---|---|---|
| A.11.1.1 | Physical security perimeter | 1 - Inicial | El servicio de seguridad externo no conoce con veracidad las normas de Seguridad de Información conocen de manera superficial la protección de la infraestructura pero no la protección de datos como tal. |
| A.11.1.2 | Physical entry controls | 2 - Repetible | Los accesos a áreas sensibles se encuentran definidos pero no son totalmente restrictivos. |
| A.11.1.3 | Securing offices, rooms, and facilities | 1 - Inicial | Los accesos a áreas sensibles se encuentran definidos pero no son totalmente restrictivos. |
| A.11.1.4 | Protecting against external and environmental threats | 0 - No existente | El plan de contingencia y de recuperación de desastres no se encuentra documentado. |
| A.11.1.5 | Working in secure areas | 0 - No existente | El control no se aplica y tampoco existe percepción de su existencia. |
| A.11.1.6 | Delivery and loading areas | 1 - Inicial | El control no se aplica y tampoco existe percepción de su existencia. |
| A.11.2 Equipment | | | |
| A.11.2.1 | Equipment siting and protection | 2 - Repetible | El control se encuentra definido más no se encuentra correctamente documentado. |
| A.11.2.2 | Supporting utilities | 2 - Repetible | El control se encuentra definido más no se encuentra correctamente documentado. |
| A.11.2.3 | Cabling security | 2 - Repetible | El control se encuentra definido más no se encuentra correctamente documentado. |
| A.11.2.4 | Equipment maintenance | 2 - Repetible | El control se encuentra definido más no se encuentra correctamente documentado. |
| A.11.2.5 | Removal of assets | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante |
| A.11.2.6 | Security of equipment and assets off-premises | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante |
| A.11.2.7 | Secure disposal or reuse of equipment | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante |
| A.11.2.8 | Unattended user equipment | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante |
| A.11.2.9 | Clear desk and clear screen policy | 0 - No existente | No existen herramientas ni procedimientos que normen este control. |
| A.12 Operations security | | | |
| A.12.1 Operational procedures and responsibilities | | | |
| A.12.1.1 | Documented operating procedures | 2 - Repetible | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| A.12.1.2 | Change management | 2 - Repetible | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| A.12.1.3 | Capacity management | 2 - Repetible | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| A.12.1.4 | Separation of development, testing and operational environments | 1 - Inicial | La empresa acoge un procedimiento intuitivo pero que no se encuentra documentado |
| A.12.2 Protection from malware | | | |
| A.12.2.1 | Controls against malware | 0 - No existente | No existen controles ni procedimientos que normen este apartado. |
| A.12.3 Backup | | | |

| | | | |
|---|---|---|---|
| A.12.3.1 | Information backup | 2 - Repetible | La empresa acoge un procedimiento intuitivo pero que no se encuentra documentado |
| A.12.4 Logging and monitoring | | | |
| A.12.4.1 | Event logging | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante ni bajo un cronograma establecido. |
| A.12.4.2 | Protection of log information | 0 - No existente | No existen herramientas ni procedimientos que normen este control. |
| A.12.4.3 | Administrator and operator logs | 0 - No existente | No existen herramientas ni procedimientos que normen este control. |
| A.12.4.4 | Clock synchronisation | 0 - No existente | No existen herramientas ni procedimientos que normen este control. |
| A.12.5 Control of operational software | | | |
| A.12.5.1 | Installation of software on operational systems | 1 - Inicial | La empresa acoge un procedimiento intuitivo pero que no se encuentra documentado |
| A.12.6 Technical vulnerability management | | | |
| A.12.6.1 | Management of technical vulnerabilities | 1 - Inicial | No existen herramientas ni procedimientos que normen este control. |
| A.12.6.2 | Restrictions on software installation | 1 - Inicial | No existen herramientas ni procedimientos que normen este control. |
| A.12.7 Information systems audit considerations | | | |
| A.12.7.1 | Information systems audit controls | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| A.13 Communications security | | | |
| A.13.1 Network security management | | | |
| A.13.1.1 | Network controls | 2 - Repetible | La empresa acoge un procedimiento intuitivo pero que no se encuentra documentado. |
| A.13.1.2 | Security of network services | 2 - Repetible | La empresa acoge un procedimiento intuitivo pero que no se encuentra documentado. |
| A.13.1.3 | Segregation in networks | 0 - No existente | No existen herramientas ni procedimientos que normen este control. |
| A.13.2 Information transfer | | | |
| A.13.2.1 | Information transfer policies and procedures | 0 - No existente | No existen controles ni procedimientos que normen este apartado. |
| A.13.2.2 | Agreements on information transfer | 0 - No existente | No existen controles ni procedimientos que normen este apartado. |
| A.13.2.3 | Electronic messaging | 0 - No existente | No existen controles ni procedimientos que normen este apartado. |
| A.13.2.4 | Confidentiality or nondisclosure agreements | 4 - Gestionado | El control se encuentra definido y se encuentra correctamente documentado. |
| A.14 System acquisition, development, and maintenance | | | |

| | | | | |
|---|---|---|---|---|
| A.14.1 Security requirements of information systems | | | | |
| | A.14.1.1 | Information security requirements analysis and specification | 2 - Repetible | La empresa acoge metodologías acordes a buenas prácticas pero no establece la implementación documentada de las mismas. |
| | A.14.1.2 | Securing application services on public networks | 2 - Repetible | Existe la percepción de la existencia del control pero no se aplica de manera constante en todos los sistemas del catálogo de servicios. |
| | A.14.1.3 | Protecting application services transactions | 2 - Repetible | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| A.14.2 Security in development and support processes | | | | |
| | A.14.2.1 | Secure development policy | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| | A.14.2.2 | System changes control procedures. | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| | A.14.2.3 | Technical review of applications after operating platform | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| | A.14.2.4 | Restrictions on changes to software packages | 0 - No existente | No existen herramientas ni procedimientos que normen este control. |
| | A.14.2.5 | Secure system engine nearing principles | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| | A.14.2.6 | Secure development environment | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| | A.14.2.7 | Outsourced development | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| | A.14.2.8 | System security testing | 2 - Repetible | La empresa acoge buenas prácticas pero no establece la implementación documentada. |
| | A.14.2.9 | System acceptance testing | 2 - Repetible | La empresa acoge buenas prácticas pero no establece la implementación documentada. |
| A.14.3 Test data | | | | |
| | A.14.3.1 | Protection of test data | 2 - Repetible | La empresa acoge metodologías acordes a buenas prácticas pero no establece la implementación documentada de las mismas. |
| A.15 Supplier relationships | | | | |
| A.15.1 Information security in supplier relationships | | | | |
| | A.15.1.1 | Information security policy for supplier relationships | 0 - No existente | No existen controles ni procedimientos que normen este apartado. |
| | A.15.1.2 | Addressing security within supplier agreements | 0 - No existente | No existen controles ni procedimientos que normen este apartado. |
| | A.15.1.3 | Information and communication technology supply chain | 0 - No existente | No existen controles ni procedimientos que normen este apartado. |
| A.15.2 Supplier service delivery management | | | | |
| | A.15.2.1 | Monitoring and review of supplier services | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| | A.15.2.2 | Managing changes to supplier services | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| A.16 Information security incident management | | | | |

| | | | | |
|---|---|---|---|---|
| A.16.1 Management of information security incidents and improvements | | | | |
| | A.16.1.1 | Responsibilities and procedures | 3 - Definido | El control está definido, el procedimiento documentado , pero no se aplica de manera constante. |
| | A.16.1.2 | Reporting information security events | 2 - Repetible | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| | A.16.1.3 | Reporting information security weaknesses | 1 - Inicial | La empresa acoge un procedimiento intuitivo pero que no se encuentra documentado. |
| | A.16.1.4 | Assessment of and decision on information security events | 2 - Repetible | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| | A.16.1.5 | Response to information security incidents | 2 - Repetible | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| | A.16.1.6 | Learning from information security incidents | 0 - No existente | No existen herramientas ni procedimientos que normen este control. |
| | A.16.1.7 | Collection of evidence | 0 - No existente | No existen herramientas ni procedimientos que normen este control. |
| A.17 Information security aspects of business continuity management | | | | |
| A.17.1 Information security continuity | | | | |
| | A.17.1.1 | Planning information security continuity | 2 - Repetible | La empresa acoge un procedimiento intuitivo pero que no se encuentra documentado. |
| | A.17.1.2 | Implementing information security continuity | 2 - Repetible | La empresa acoge un procedimiento intuitivo pero que no se encuentra documentado. |
| | A.17.1.3 | Verify, review, and evaluate information security continuity | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| A.17.2 Redundancies | | | | |
| | A.17.2.1 | Availability of information processing facilities | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| A.18 Compliance | | | | |
| A.18.1 Compliance with legal and contractual requirements | | | | |
| | A.18.1.1 | Identification of applicable legislation and contractual requirements | 0 - No existente | No existen controles ni procedimientos que normen este apartado. |
| | A.18.1.2 | Electoral property rights | 0 - No existente | No existen controles ni procedimientos que normen este apartado. |
| | A.18.1.3 | Protection of records | 0 - No existente | No existen controles ni procedimientos que normen este apartado. |
| | A.18.1.4 | Privacy and protection of personally identifiable information | 0 - No existente | No existen controles ni procedimientos que normen este apartado. |
| | A.18.1.5 | Regulation of cryptographic controls | 0 - No existente | No existen controles ni procedimientos que normen este apartado. |
| A.18.2 Information security reviews | | | | |
| | A.18.2.1 | Independent review of information security | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| | A.18.2.2 | Compliance with security policies and standards | 1 - Inicial | Existe la percepción de la existencia del control pero no se aplica de manera constante. |
| | A.18.2.3 | Technical compliance review | 0 - No existente | No existen controles ni procedimientos que normen este apartado. |

*Tabla 3 - GAP, Estado de los controles.*

## 1.6 Resultados

Luego del análisis diferencial realizado es necesario indicar que la situación actual de la organización respecto a Seguridad de la información es bastante precaria en términos generales, ya que a pesar de conocer su importancia no existen procedimientos ni estrategias que normen la mayoría de los controles. Por lo que los resultados de nuestro GAP se reflejan en la siguiente tabla de puntajes y gráfico de análisis.

| DOMINIO | Valor |
|---|---|
| A.5 Information security policies | **1** |
| A.6 Organization of information security | **0,7** |
| A.7 Human resource security | **0,5** |
| A.8 Asset management | **1,111** |
| A.9 Access control | **1** |
| A.10 Cryptography | **0** |
| A.11 Physical and environmental security | **1,5** |
| A.12 Operations security | **1,048** |
| A.13 Communications security | **1,167** |
| A.14 System acquisition, development, and maintenance | **1,704** |
| A.15 Supplier relationships | **0,5** |
| A.16 Information security incident management | **1,429** |
| A.17 Information security aspects of business continuity management | **1,333** |
| A.18 Compliance | **0,333** |

*Tabla 4 - Puntaje análisis GAP.*

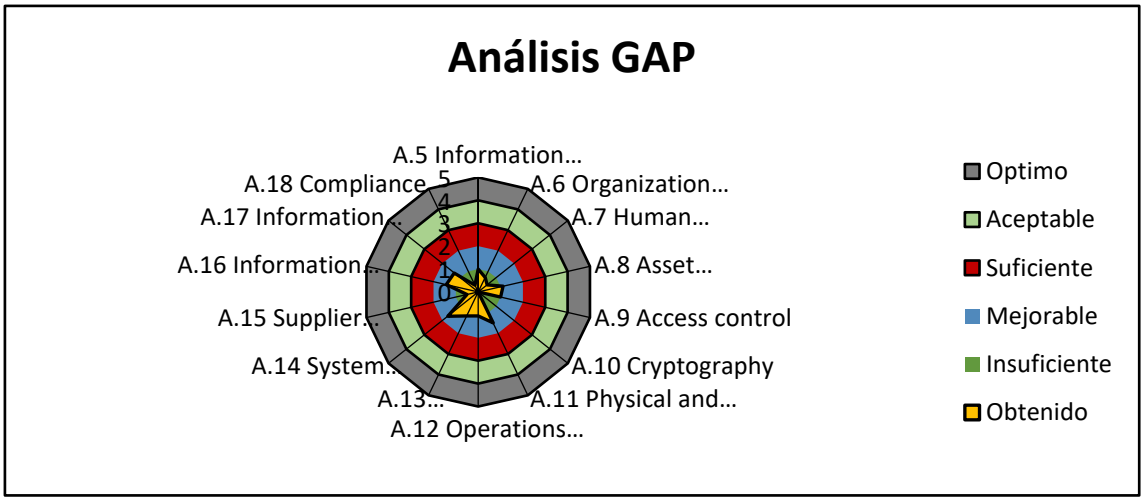



*Ilustración 4 - Análisis GAP.*

# 2. Sistema de Gestión Documental.

## 2.1 Introducción.

## 2.2 Esquema Documental.

### 2.2.1 Política de Seguridad.

**OBJETIVO.**
Normar y controlar la gestión de la seguridad de la información institucional, en todo su ciclo de vida y formatos, con el propósito de proteger la información mediante la implementación de medidas de seguridad preventivas, detectoras, de respuesta, y de recuperación, que contribuyan a garantizar la confidencialidad, integridad y disponibilidad de la información física y digital; gestión que a su vez debe estar alineada al cumplimiento de los objetivos institucionales.

**ALCANCE.**
La presente normativa se aplica para la protección de toda la información física o digital, recibida o generada durante los procesos gobernantes, habilitadores de asesoría, habilitadores de apoyo y flujo que realiza la EMPRESA PÚBLICA AGUAS DE MANTA, así como la información que se encuentra bajo custodia de los servidores de la institución durante su proceso de atención de trámites y en archivos físicos, temporales o permanentes, bases de datos, almacenada en recursos tecnológicos a nivel de usuario y equipos servidores; y, la información que se encuentra en etapa de gestión de procesos internos.

**DESCRIPCIÓN DE LA POLÍTICA**
**BASE LEGAL**

- Constitución de la República del Ecuador (Decreto Legislativo 0. Registro Oficial 449 de 20-oct-2008. Última modificación: 13-jul-2011).

- Ley Orgánica de Servicio Público, LOSEP (Ley 0. Registro Oficial Suplemento 294 de 06-oct-2010).

- Registro oficial N°41 Creación Empresa Pública Aguas de Manta.

- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 2002-67).

- Ley Orgánica de Transparencia y Acceso a la Información Pública No.24. (Registro Oficial Suplemento 337 de 18-may-2004).

- Reglamento General a la Ley Orgánica del Servicio Público (Decreto Ejecutivo 710. Registro Oficial Suplemento 418 de 01-abr-2011. Última modificación: 10-oct-2011).

- Acuerdo No. 025-2019, Esquema Gubernamental de Seguridad de la Información EGSI (10 de enero de 2020).

- Norma Técnica ISO/IEC 27001:2013 TECNOLOGÍAS DE LA INFORMACIÓN — TÉCNICAS DE SEGURIDAD — SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – REQUISITOS.

- Norma Técnica ISO/IEC 27002:2013 CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

**NORMAS Y DISPOSICIONES GENERALES**

a) Las normas generales de este documento son de aplicación obligatoria para todos los servidores de la EMPRESA PÚBLICA AGUAS DE MANTA, en tanto guarden conformidad con las disposiciones legales, reglamentarias y resoluciones vigentes al momento de ejecutarse el respectivo procedimiento. En el caso de cambios o modificaciones en dicho marco normativo, tales normas vigentes prevalecen sobre las disposiciones aquí contenidas.

b) El personal que incumpliere sus obligaciones o contraviniere las disposiciones de esta Política, así como las leyes y normativa conexa, incurren en responsabilidad administrativa que será sancionada disciplinariamente, sin perjuicio de la acción civil o penal que pudiere originar el mismo hecho.

c) La EMPRESA PÚBLICA AGUAS DE MANTA es responsable de la protección y custodia de la información Institucional recibida o generada por el personal interno y/o externo autorizado en la utilización de los distintos sistemas administrativos, aplicaciones informáticas y/o servicios tecnológicos asignados para el cumplimiento de sus funciones, atención de trámites y transacciones asociadas a su gestión; la misma podrá estar contenida en documentos, informes, reportes, bases de datos, archivos temporales o permanentes sean estos físicos o digitales, los cuales son sujeto de custodia y control de la EMPRESA PÚBLICA AGUAS DE MANTA.

d) La norma ecuatoriana denominada como Esquema Gubernamental de Seguridad de la Información (EGSI) considera el diseño, implantación, mantenimiento de un conjunto de procesos y políticas para gestionar eficientemente la accesibilidad de la información y garantizar la confidencialidad, integridad y disponibilidad de esta, minimizar a la vez los riesgos de seguridad de la información, mediante un conjunto de protecciones, controles, medidas preventivas y reactivas.

e) La entrega de información por parte del EMPRESA PÚBLICA AGUAS DE MANTA a otras Instituciones del Estado y entidades externas, se realizará conforme a los respectivos convenios, acuerdos de reserva de información y criterios de confidencialidad que se determinen para el efecto.

f) Todos los aspectos que no se encuentren normados de forma expresa en esta Política deben ser complementados o suplidos por el marco normativo vigente.

## ASPECTOS ORGANIZATIVOS DE LA GESTIÓN DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN.

a) La Gerencia de Tecnología de Información y Comunicación, administra los recursos tecnológicos institucionales, para garantizar la seguridad de la información digital y de los recursos tecnológicos que administra.

b) Corresponde a esta Gerencia la identificación y mitigación de los riesgos tecnológicos y de seguridad de los activos de información en el ámbito de su competencia.

c) El acceso a los servicios tecnológicos de información y comunicación, que son proporcionados a los funcionarios de la Empresa Pública Aguas de Manta EPAM, deberán utilizarse para los propósitos relacionados con las actividades de la institución.

## CLASIFICACIÓN DE LA INFORMACIÓN INSTITUCIONAL.

a) **Grupo de Información,** es el conjunto de datos o documentos físicos que tienen características comunes de agrupación, y que conforman una unidad de información independiente, tales como: base de datos, información de proyectos, expedientes de RRHH, etc.

b) **Información general,** es aquella creada en los procesos administrativos, financieros, tecnológicos y de control del EMPRESA PÚBLICA AGUAS DE MANTA.

c) **Información de Alta criticidad,** es la información sujeta a restricción, con acceso restringido a un número limitado de servidores autorizados por la institución.

d) **Información de baja criticidad ,** es la información general, con acceso de lectura únicamente a los servidores de la EMPRESA PÚBLICA AGUAS DE MANTA, y personal externo autorizado; incluyendo en este nivel, toda información correspondiente a documentos que contengan metodologías o mejores prácticas para la ejecución de

actividades internas, así como documentos que engloban políticas, procedimientos, instructivos, formatos, guías operativas.

e) **Información No Critica**, son los datos, grupos de datos o información declarada de conocimiento público, la cual se encuentra expuesta a terceros o puede entregarse masivamente en formato digital o físico sin restricciones a cualquier persona o entidad, interna o externa

f) El uso y acceso a la información institucional contenida en los repositorios centrales de almacenamiento deben estar restringidos según el nivel de sensibilidad de la información y aplicación de las medidas de protección que corresponda.

g) Para compartir la información institucional que se encuentre almacenada en los repositorios centrales, se debe aplicar el principio de "menor privilegio", el cual determina que todos los usuarios autorizados deben tener asignados la cantidad mínima de privilegios y permisos a la información institucional, que permita el desarrollo normal de sus funciones.

h) **Custodios de la información institucional**, es el personal de la Institución que usa o resguarda temporal o permanentemente la información durante su vinculación laboral, para lo cual debe aplicar las medidas de protección requeridas.

i) Para el manejo de información sensitiva alta o baja, es obligación del personal de la Institución y personal externo autorizado:

1. Utilizar la información a la que tiene acceso debido a sus funciones, únicamente para los fines permitidos, conforme a la normativa y a las órdenes de su superior jerárquico.

2. Abstenerse de acceder a la información no autorizada, no asignada o no permitida.

3. No revelar, disponer, guardar, extraer, archivar, reproducir o eliminar información con fines ajenos al ejercicio específico de sus funciones.

4. No utilizar la información para provecho o ventaja personal, familiares, o cualquier otra persona, ni en perjuicio de terceros.

5. Aplicar las medidas de protección que sean necesarias para proteger la información institucional, a fin de minimizar el riesgo de difusión, acceso y uso no autorizado,

para evitar impacto negativo a la imagen y gestión de la Institución y/o en perjuicio de la EMPRESA PÚBLICA AGUAS DE MANTA, responsables o terceros.

6. Mantener las estaciones de trabajo libres, evitando exponer documentos físicos y/o dispositivos tecnológicos que contengan información Institucional.

**USO ACEPTABLE DE COMPUTADORES Y DISPOSITIVOS DE MANEJO DE INFORMACIÓN.**

a) La EMPRESA PÚBLICA AGUAS DE MANTA declara y establece que los computadores de escritorio y/o portátiles, así como los recursos y servicios configurados en dichos equipos, son de su propiedad, los mismos que facilitan la gestión y custodia de la información institucional; por lo tanto, deben ser tratados como activos institucionales, sujetos de administración y control, de conformidad con los procedimientos de control respectivos.

b) Toda la información almacenada en los computadores de escritorio y/o portátiles asignados al personal de la Institución, es de propiedad de la EMPRESA PÚBLICA AGUAS DE MANTA, motivo por el cual debe ser monitoreada y controlada.

c) La autorización y uso de dispositivos de almacenamiento externo se debe realizar conforme a la normativa vigente.

d) El personal de la EMPRESA PÚBLICA AGUAS DE MANTA, y personal externo autorizado, a quienes se les haya asignado un computador de escritorio y/o portátil de la Institución, deben cumplir las siguientes normas:

2. Acatar las normas establecidas para la generación y uso de contraseñas relacionadas con computadores de escritorio y portátiles.

3. La información sensitiva alta almacenada en computadores portátiles debe estar encriptada utilizando las herramientas Institucionales definidas para este efecto.

4. Todo computador o dispositivo institucional que haya cumplido su vida útil, y que, por efecto de disposición legal, se done o destruya, debe previamente ser formateado y sanitizado de manera segura, para evitar que información institucional sensible o no sensible, se vea comprometida.

**USO ACEPTABLE DE SERVICIOS Y/O RECURSOS TECNOLÓGICOS.**

a) Los servicios y/o recursos tecnológicos que la EMPRESA PÚBLICA AGUAS DE MANTA asigna al personal de la Institución y personal externo autorizado para el cumplimiento de sus funciones, debe ser utilizado únicamente para este fin.

b) La EMPRESA PÚBLICA AGUAS DE MANTA se reserva el derecho de habilitar, deshabilitar, ampliar o restringir los servicios y/o recursos tecnológicos, al personal interno o externo, como medidas para asegurar el uso aceptable de los mismos y la seguridad de la información institucional.

c) Todos los computadores de escritorio y/o portátiles asignados por la EMPRESA PÚBLICA AGUAS DE MANTA al personal de la Institución y personal externo autorizado, deben tener instalado y operativo el antivirus institucional para protegerlo contra amenazas de código malicioso.

d) La asignación de tokens con certificados de firma electrónica para el personal de la EMPRESA PÚBLICA AGUAS DE MANTA autorizado para su utilización, deben cumplir el procedimiento establecido conforme a la normativa vigente.

e) Los repositorios centrales de almacenamiento de información digital institucional deben ser utilizados exclusivamente para guardar información relacionada a las funciones que cumplen el personal de la Institución, personal externo autorizado. El uso y acceso a la información institucional contenida en los repositorios centrales de almacenamiento deben estar restringidos según el nivel de sensibilidad de la información y aplicación de las medidas de protección. La administración técnica de los repositorios centrales de almacenamiento está bajo la responsabilidad de la Gerencia de Tecnologías de la Información y Comunicación.

**USO ACEPTABLE DEL SERVICIO DE CORREO ELECTRÓNICO INSTITUCIONAL.**

a) El servicio de correo electrónico institucional interno es asignado a todo el personal que deba interactuar a través de la red de datos institucional; el servicio se debe habilitar atendiendo a las necesidades del personal que lo requiera para el cumplimiento de sus funciones.

b) El servicio y las cuentas de correo electrónico institucional que se encuentran bajo los dominios “@epam.gob,ec” y “@aguasdemanta.gob.ec”, son de propiedad de la EMPRESA PÚBLICA AGUAS DE MANTA.

c) El despliegue detallado de estas normas para el uso aceptable y adecuado del servicio institucional del correo electrónico constará en la Política “Uso de Correo Electrónico” emitida para tal efecto.

**USO ACEPTABLE DEL SERVICIO DE INTERNET.**

a) La Gerencia de Tecnologías de la Información y Comunicación define las categorías y grupos de navegación del servicio de internet institucional, así como su implementación y despliegue.

b) La asignación de permisos y accesos adicionales será verificada y aprobada bajo el previo el análisis de la Gerencia de Tecnologías de la Información y Comunicación, en base a las necesidades del requirente y considerando la naturaleza de sus funciones.

c) El uso aceptable y adecuado del servicio institucional de Internet constará en la Política "Uso de Internet" emitida para tal efecto.

**INCIDENCIA DEL RECURSO HUMANO.**

a) El personal de la EMPRESA PÚBLICA AGUAS DE MANTA debe difundir y declarar el entendimiento y compromiso de las normas de la presente Política, a través del conocimiento y aceptación del acuerdo de responsabilidades sobre Reserva y Confidencialidad de la Información, y los mecanismos que se establezcan para la contratación y selección de personal.

b) El personal externo autorizado debe manifestar el compromiso de cumplimiento de las normas de seguridad de la información, a través de los respectivos contratos u acuerdos que defina la EMPRESA PÚBLICA AGUAS DE MANTA para este efecto.

c) Las Gerencias deben solicitar la asignación al personal a su cargo, los perfiles y roles de acceso a la información mínimos que correspondan a través de las aplicaciones informáticas institucionales, así como los servicios y recursos tecnológicos necesarios para el cumplimiento de sus funciones y responsabilidades.

d) Al término de la relación laboral de un servidor, la respectiva Gerencia debe gestionar la recepción de la información institucional a cargo del servidor saliente, lo cual debe estar establecido como un insumo preponderante antes de llevar a cabo la "Liquidación de Haberes".

**SEGURIDAD FÍSICA DE LA INFORMACIÓN INSTITUCIONAL.**

a) La Gerencia de Tecnologías de la Información y Comunicación y la EMPRESA PÚBLICA AGUAS DE MANTA, en el ámbito de sus competencias, deben gestionar la implementación de las seguridades físicas tanto perimetrales como internas, a fin de salvaguardar de manera correcta la información digital. Esta gestión establecerá los

controles de acceso y las medidas de protección contra amenazas externas o ambientales.

b) La Gerencia de Tecnologías de la Información y Comunicación y la EMPRESA PÚBLICA AGUAS DE MANTA, deberán documentar y aprobar un plan de contingencia contra desastres.

## CORRECTO USO DE LA GESTIÓN DE COMUNICACIONES, IMPLEMENTACIÓN Y OPERACIONES.

*DISPONIBILIDAD DE LOS SERVICIOS Y RECURSOS TECNOLÓGICOS.*

a) La Gerencia de Tecnologías de la Información y Comunicación debe implementar los mecanismos y controles necesarios para garantizar la disponibilidad de los servicios y recursos tecnológicos institucionales.

*SEGURIDAD PERIMETRAL Y DE TELECOMUNICACIONES.*

a) La Gerencia de Gerencia de Tecnologías de la Información y Comunicación autoriza y administra los accesos a los diferentes ambientes y servidores (producción, base de datos, desarrollo, pruebas)

b) Todos los permisos autorizados e implementados en los firewalls institucionales están sujetos a monitoreo y control por parte de la Gerencia de Tecnologías de la Información y Comunicación.

c) La Gerencia de Tecnologías de la Información y Comunicación, debe realizar la depuración permanente de los accesos habilitados en el firewall y publicaciones de servicios que existieren.

d) La Gerencia de Tecnologías de la Información y Comunicación debe implementar herramientas de control, detección, prevención y recuperación para proteger la plataforma tecnológica contra código malicioso.

*RESPALDOS DE INFORMACIÓN INSTITUCIONAL.*

a) La Gerencia de Tecnologías de la Información y Comunicación debe documentar un plan de despliegue ante las necesidades de respaldo de información y/o configuración de las bases de datos y ficheros que administra.

b) Las condiciones de respaldo de la información serán ejecutadas conforme a la Política “Gestión y Respaldo de la Información” y procedimientos establecidos para el efecto.

*SEGURIDAD LÓGICA DE LA INFORMACIÓN INSTITUCIONAL.*

a) Para los accesos a la red de datos y a la infraestructura tecnológica de la EMPRESA PÚBLICA AGUAS DE MANTA, se debe establecer mecanismos de autenticación que garanticen la identificación del personal de la Institución y/o personal externo debidamente autorizado, al igual que de los computadores de escritorio y/o portátiles y equipos periféricos de la infraestructura tecnológica de la institución, de acuerdo con lo establecido en el procedimiento conforme la normativa vigente.

b) El personal de la Institución y personal externo que tenga autorizado el acceso, local o remoto a la infraestructura tecnológica de la EMPRESA PÚBLICA AGUAS DE MANTA, desde las redes cableadas o inalámbricas, a través de computadores de escritorio o portátiles, debe tener asignado un perfil con los accesos de red necesarios, asociados a la cuenta de red creada para el efecto.

c) El Control de Accesos Lógicos se basa en la creación de usuarios específicos y únicos que deben ser asignados al personal de la Institución que requieran acceso a la infraestructura tecnológica y/o aplicaciones informáticas de la Secretaria Técnica de Mar.

d) El uso de cuentas individuales o genéricas es intransferible; para el caso de cuentas genéricas estas deben ser asignadas y registradas a un servidor de la Institución responsable de la misma.

e) El acceso a la información institucional que tenga el personal externo que preste servicios al EMPRESA PÚBLICA AGUAS DE MANTA, debe estar regulada por los respectivos contratos y acuerdos de confidencialidad que se suscriban para el efecto.

f) Cuando un usuario finalice su relación laboral y/o contractual con la Institución, el Administrador de Accesos debe proceder a la inhabilitación inmediata y definitiva del usuario de red, aplicaciones informáticas, servicios y recursos tecnológicos, así como la revocatoria de los respectivos perfiles, roles, y privilegios que tenía autorizado, de acuerdo con lo establecido en los procedimientos vigentes.

g) Para la asignación de accesos, permisos, derechos, o privilegios, dentro de los sistemas informáticos, bases de datos, servicios y recursos tecnológicos, componentes de la plataforma/infraestructura tecnológica, se debe aplicar el principio del menor privilegio.

h) La administración de los componentes de la plataforma tecnológica es responsabilidad exclusiva del personal técnico perteneciente a la Gerencia de Tecnologías de la Información y Comunicación. Toda actividad de administración o monitoreo de los diferentes componentes de la infraestructura tecnológica debe ser realizada utilizando

las cuentas de usuario individual (no genérica) asignadas a cada administrador de la plataforma tecnológica. En aquellos casos que técnicamente se requiera una cuenta genérica para administrar un recurso de la infraestructura tecnológica, se lo puede efectuar siempre que se identifique administrativamente al responsable de esta.

i) El acceso a la infraestructura de red y seguridad informática institucional está autorizado a los administradores tecnológicos respectivos con fines de administración, con objetivo de monitoreo y control.

j) Se debe controlar los accesos locales y remotos de todos los usuarios a la infraestructura tecnológica de la EMPRESA PÚBLICA AGUAS DE MANTA, por parte del personal de la Institución y personal externo autorizado, a través de mecanismos de autorización y autenticación que deben ser definidos y administrados por la Gerencia de Tecnologías de la Información y Comunicación.

k) La gestión de cuentas de administración local de los computadores de escritorio o portátiles asignados a los usuarios finales autorizados, debe estar a cargo de la Gerencia de Tecnologías de la Información y Comunicación y deben ser utilizadas únicamente para brindar soporte en sitio por parte del personal técnico autorizado.

### *ADQUISICIÓN, DESARROLLO, PUESTA EN PRODUCCIÓN Y MANTENIMIENTO DE APLICACIONES INFORMÁTICAS.*

a) En el desarrollo, mantenimiento y adquisición de aplicaciones informáticas, se debe implementar controles y acciones que garanticen la disponibilidad de los sistemas y aplicativos informáticos institucionales, para lo cual se debe considerar la línea base de seguridad establecida para aplicaciones informáticas elaborada por la Gerencia de Tecnologías de la Información y Comunicación.

b) Periódicamente se deben ejecutar evaluaciones de cumplimiento de las medidas y controles de seguridad en las aplicaciones informáticas. En caso de encontrar vulnerabilidades en las aplicaciones informáticas, las mismas deben ser corregidas y se deben implementar los controles correspondientes por parte de la Gerencia de Tecnologías de la Información y Comunicación.

c) La Gerencia de Tecnologías de la Información y Comunicación, debe llevar y actualizar el inventario de las aplicaciones de software licenciado, software o herramientas de uso libre, demos, software con licencias temporales, que sean utilizadas en la EMPRESA PÚBLICA AGUAS DE MANTA; conforme a la normativa vigente.

d) El repositorio de software debe contener los instaladores del software autorizado para ser utilizado como único mecanismo, para la instalación de software adicional en los

computadores de escritorio y/o portátiles, actividad que está a cargo de la Gerencia de Tecnologías de la Información y Comunicación.

e) La instalación de cualquier software adicional sea este licenciado o de uso libre, en los computadores de escritorio o portátiles, y en equipos servidores, está autorizado para los servidores que lo requieran para la ejecución de sus tareas en la Institución, siempre y cuando se cumpla con las autorizaciones que correspondan.

*RESTRICCIONES Y PROHIBICIONES.*

a) Se prohíbe expresamente lo siguiente:

- Usar los recursos físicos y tecnológicos de la EMPRESA PÚBLICA AGUAS DE MANTA para, almacenar, acceder, transmitir o difundir la siguiente información o material:

  - Textos o imágenes pornográficas.
  - Que promueva de cualquier forma la explotación sexual, racismo o violencia.
  - Que promueva el uso ilegal de drogas o armas.
  - Mensajes discriminatorios con relación a ideología, afiliación política o sindical, orientación sexual, etnia, religión, nacionalidad, condición migratoria.
  - Con contenido violento.
  - Que promueva o posibilite juegos o apuestas.
  - Que contenga cualquier tipo de código malicioso (virus, programas que se auto replican, programas espías, programa de captura de credenciales, etc.).
  - Que intente vulnerar la seguridad de las aplicaciones, servicios o equipos de propiedad de la EMPRESA PÚBLICA AGUAS DE MANTA.
  - Correos masivos, cadenas de correos, spam.
  - Que incluya texto difamatorio, ofensivo, intimidatorio o injurioso contra la honra de las personas.
  - Que atente contra los derechos de autor, y no posean licencias.

b) Para el uso de equipos, servicios y recursos tecnológicos institucionales se prohíbe:

- Instalar software adicional no autorizado.

- Cambiar o intentar cambiar las configuraciones de los equipos asignados, incluyendo CMOS, BIOS, sistema operativo, aplicativos y herramientas del computador.

- Abrir físicamente el computador, bajo ningún concepto. Cualquier actividad técnica debe ser coordinada con el personal de soporte a usuarios.

- Está prohibido almacenar, transmitir o reenviar mensajes de datos, incompatibles con los estándares éticos del personal de la Institución de la EMPRESA PÚBLICA AGUAS DE MANTA, y con las normas legales o reglamentarias aplicables.

- Utilizar el servicio de correo electrónico institucional para divulgar o transmitir información institucional de propiedad de la EMPRESA PÚBLICA AGUAS DE MANTA, a terceras personas u organizaciones no autorizadas.

- Transmitir información institucional considerada como de alta criticidad a través de mensajes de datos, sin haber recibido la autorización respectiva para la entrega de información.

- Acceder al archivo de correo o a una cuenta de correo electrónico institucional que pertenezca a otro servidor, personal externo autorizado, sin su autorización expresa o de la autoridad competente.

- Alterar el contenido de los mensajes de datos que modifiquen la voluntad, intención u objetivo del remitente original para a su vez reenviar el mensaje de datos alterado, violentando el principio de integridad de la información.

- Incumplir con lo establecido para uso aceptable y adecuado de contraseñas establecido en la Política “Uso de Contraseñas” emitida para tal efecto.

- Enviar mensajes alterando la dirección electrónica del remitente para suplantar la identidad, identificarse como una persona ficticia o no identificarse.

- Intentar vulnerar las seguridades de los diferentes sistemas, accesos a red, internet y del servicio de correo electrónico institucional.

- Usar frases o palabras obscenas, peyorativas, ofensivas o denigrantes en los mensajes de correo electrónico institucional.

## *GLOSARIO DE TÉRMINOS.*

- **Activos de Información:** Son ficheros y bases de datos, contratos y acuerdos, documentación institucional, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos y servicios informáticos y de telecomunicaciones.

- **Código Malicioso:** Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario.

- **Confidencialidad:** Condición que garantiza que la información institucional sea accesible solo al personal autorizado a tener acceso a la misma, y que ésta no debe ser revelada de forma no autorizada.

- **Contraseña**. - Es una serie secreta de caracteres que permite a un usuario autenticarse y tener acceso, entre otros a: sistemas de información, redes, bases de datos, servicios, o recursos tecnológicos.

- **Controles**: Consisten en todos los métodos y mecanismos físicos como tecnológicos, políticas y procedimientos de la Institución, creados con el objetivo de asegurar protección y buen uso de sus activos de información, garantizar la exactitud y fiabilidad de sus registros, y el cumplimiento operativo de las normas corporativas.

- **Custodios de la información institucional**: Son el personal que usan o resguardan temporal o permanentemente la información durante su vida útil.

- **Disponibilidad**: Condición que garantiza que los usuarios autorizados tengan acceso a la información institucional y a los recursos relacionados con la misma, toda vez que lo requieran de acuerdo con las funciones asignadas.

- **Grupo de Información**: Son conjuntos de datos o documentos físicos que tienen características comunes de agrupación, y que conforman una Gerencia de información independiente.

- **Información**: Conjunto organizado de datos significativos y procesados, que sirven a un objetivo específico, y cuyo uso racional constituye la base para la toma de decisiones, resolución de problemas, gestión de procesos, y gestión del conocimiento

- **Información Digital**: Es toda información generada y procesada por equipos electrónicos de cómputo, y almacenada en dispositivos ópticos y medios magnéticos

como discos duros, discos externos, USB, CD/DVD, Pendrive, Tablet-PC, IPad, teléfonos inteligentes, etc.

- **Información Física**: Es toda información impresa o escrita en papel, sea documentos, oficios, memorandos, informes, reportes.

- **Información Institucional**: Es toda información digital o física, recibida o generada como parte de la ejecución de los procesos estratégicos, operativos y de apoyo de la EMPRESA PÚBLICA AGUAS DE MANTA, así como la información relacionada con la correspondencia, y que se encuentra almacenada física o digitalmente; o la información que se encuentre en etapa de gestión en los procesos internos.

- **Integridad**: Condición que garantiza la exactitud y totalidad de la información institucional.

- **Medidas de protección**: Conjunto de acciones físicas, técnicas, normativas y organizativas que se orientan a garantizar la confidencialidad, integridad y disponibilidad de la información institucional y que deben adoptarse en función del nivel de sensibilidad de la información.

- **Personal de la Institución**: Son todas las personas que trabajen, presten servicios o ejerzan un cargo, función o dignidad dentro de la EMPRESA PÚBLICA AGUAS DE MANTA.

- **Personal externo autorizado**: Es toda persona natural que actúe a cuenta propia o en representación de una persona jurídica, que tenga relación contractual con el EMPRESA PÚBLICA AGUAS DE MANTA

- **Riesgo**: Es un evento de incertidumbre, que si llega a ocurrir tendría un efecto que impactaría adversamente sobre la ejecución y marcha de los procesos institucionales, o sobre su resultado, afectando negativamente a la misión, visión, planes estratégicos, y objetivos institucionales.

*REVISIÓN DE LA POLÍTICA.*

Para garantizar la vigencia de la política de seguridad de la información en la institución, esta deberá ser revisada anualmente o cuando se produzcan cambios significativos a nivel operativo, tecnológica, económico, entre otros.

### 2.2.2 Procedimiento de Auditorías Internas.

**1) Objetivo.**

El presente procedimiento detalla un esquema de pasos ordenados para llevar a cabo el proceso de auditoría interna del tratamiento de la información y sistemas informáticos inmersos en la gestión institucional, desde la planificación y diseño hasta su ejecución y difusión de resultados.

Las auditorías internas de seguridad de información validan si los diversos elementos del sistema de gestión de la calidad de la organización son conformes con los requisitos dictados por la norma ISO/IEC 27001 :2013 y sus normas anexas aplicables.

**2) Alcance.**

Este procedimiento aplica desde la identificación de todos los productos tecnológicos inmersos en el Sistema de gestión de Seguridad información ofertados por la Gerencia de Tecnologías de la Información, tales como sistemas de información sujetos a control interno, soluciones de redes e infraestructura auditable en general, hasta la emisión de un informe periódico o por demanda del monitoreo efectuado.

**3) Referencias.**

Para la elaboración de este documento se consideraron los criterios establecidos en:

- Normas ISO/IEC 27001 :2013 capítulo 9.2 Auditoría Interna.
- Normas ISO/IEC 27002 :2013 capítulo 12.7 Consideraciones sobre la auditoría de sistemas de información.

**4) Responsables**

- Gerente General.
- Oficial de Seguridad.
- Gerente de Tecnología de Información y Comunicación.
- Auditores designados.
- Profesionales designados.

**5) Desarrollo.**

**5.1. Programación de Auditorias**

El Oficial de Seguridad de la organización tendrá la responsabilidad de preparar un "Programa Anual de auditoría del SGSI" (formato anexo. PDSI-FOR-001). El programa debe cubrir todos los controles del anexo A ISO/IEC 27001:2013 por lo menos una vez en el lapso de 3 años, aunque algunas soluciones o sistemas pueden ser auditados con mayor frecuencia dependiendo de:

- El estado , la importancia de los procesos o las áreas inmersas.
- Los resultados y recomendaciones de auditorías anteriores.

El "Programa Anual de auditoría del SGSI" (PDSI-FOR-001) es presentado al Gerente General para su respectiva aprobación. Este programa puede ser modificado por pedido del Oficial de seguridad y con la autorización del Gerente General, de acuerdo con las necesidades o circunstancias que se presenten.

### 5.2. Plan de Auditorias.

- El Oficial de seguridad elaborará el "Plan de Auditoría del SGSI" (SG-RG-07) antes de cada auditoria y lo comunica al Auditor Líder. El plan especifica los controles o sistemas a auditar, la fecha, la hora, contraparte/auditado y el equipo auditor designado.

  *NOTA 1:* Los auditores no deben auditar su propio trabajo o entorno donde se desempeña.

  *NOTA 2:* Están calificados como auditores internos de SGSI los miembros de la organización que cumplan con los siguientes requisitos:

- Adicionalmente, para ser auditor líder se requiere que haya participado en al menos una auditoria como parte de un equipo auditor.
- Se considera que el personal que los miembros del equipo Auditor deben cumplir los siguientes criterios de competencia:

  a.- Educación: Técnico Superior Universitario, Profesional Universitario y con antigüedad mínimo un año en la organización.

  b.- Formación: Los auditores internos y líderes deben contar con una especialización certificada en seguridad de información.

  c.- Conocimientos y Habilidades: Conocimientos de la norma ISO/IEC 27001 :2013.

  d.- Comportamiento Personal: Ético, de mentalidad abierta, observador, perceptivo, versátil, tenaz, decidido, seguro de sí mismo, actuar con fortaleza, abierto a la mejora y colaborador.

Una vez elaborado el plan, el oficial de seguridad lo comunica a los responsables correspondientes y al grupo de auditores.

### 5.3. Preparación de la Auditoría.

**Responsabilidades del auditor líder**

El auditor líder se prepara para cada auditoria de la siguiente manera:

- Revisión y Documentación exhaustiva acerca de informes anteriores de auditorías (en caso de existir).
- Revisión del plan y programación de auditorías.
- Preparación una lista de verificación en cuanto a requisitos preestablecidos (si lo considera necesario).

### 5.4. EJECUCIÓN DE LA AUDITORIA.

Previo al kick-off de la auditoría se realiza una reunión inicial, en donde se señalan los grupos de auditores que revisan cada control o SI , con la finalidad de establecer las siguientes tareas:

- Determinar el alcance.
- Presentación y aprobación de la propuesta de alcance.
- Firmas de acuerdos de confidencialidad.
- Recepción oficial de la carta de auditoría.
- Determinación del itinerario de pruebas.

Durante la auditoría, se recomienda:

- Recolección de información previa.
- Recolección objetiva de evidencias.
- Mantener retroalimentado periódicamente al auditado.
- Ejecución de pruebas sobre controles y SI.
- Análisis de resultados.

Posterior a la auditoría se establecerá una reunión para socializar los resultados de la auditoria y hacer la entrega formal del producto final del proceso, esquematizando de manera didáctica el flujo del proceso y su finalización obtenida. El propósito fundamental de esta reunión es explicar el proceso completo del desarrollo de la auditoria, realizando una breve descripción de las No Conformidades.

La auditoría se llevará a cabo de acuerdo con lo establecido en el presente Procedimiento. Puesto que la finalidad de la auditoria es la mejora continua del SGSI.
Es necesario enfocar esfuerzos en la corrección de aquellas deficiencias detectadas en auditorias anteriores, o a través de cualquier otro medio. Asimismo, se auditará la efectividad de las medidas recientemente implementadas para el SGSI.

Para fines de comprensión general de lo detallado anteriormente se propone el siguiente esquema:

| ITEM | DESCRIPCIÓN | DETALLE |
|---|---|---|
| 1 | Reunión Inicial. (Kick-off) | La auditoría se inicia con una reunión de apertura donde se confirme el ámbito de la auditoria, el programa y todo lo referente a la documentación habilitante. |
| **2** | **Ejecución.** | 1-Durante el trascurso de la auditoria debe estar presente el responsable o persona del área a auditar que facilite las evidencias objetivas y datos necesarios solicitados por el auditor para el cumplimiento satisfactorio de las actividades con la documentación aplicable. |
| | | 2- El auditor documenta la identificación de los puntos comprobados. |
| | | 3- A través de las entrevistas, observación de actividades desarrolladas, el equipo auditor busca evidencias objetivas que constaten las |

| | | |
|---|---|---|
| | | actividades auditadas según lo establecido en el SGSI. |
| | | 4- Las No Conformidades detectadas en el transcurso de la auditoria, se comenta y se analizan con el auditado: Causas que producen la No Conformidad , Los Efectos o incidencias sobre la calidad del trabajo. |
| | | 5- Las No Conformidades detectadas deben estar documentadas de forma precisa y concisa y basarse en datos objetivos. |
| 3 | Reunión Final . | 6- Durante la Auditoria se realiza una comprobación y seguimiento de la implementación y efectividad de las acciones correctivas y preventivas, pendientes de auditorías anteriores y que afecten al SGSI. |
| | | 7.-Al término de la Auditoria se realiza una reunión con la finalidad de informar resultados, en la que además del equipo auditor asiste el Oficial de Seguridad y el Gerente General. |

Tabla 5 - Pasos Ejecución de la auditoria.

### 5.5. INFORME DE AUDITORÍA

El Auditor Líder prepara el "Informe de auditoría" (PDSI-FOR-002), los mismos los deben presentar en un tiempo máximo de 45 días laborables después de la Auditoría.

Para las normas ISO, en el informe detalla los elementos auditados en todas las fases del SGSI y clasifica lo descubierto bajo los siguientes criterios:

- Fortaleza: Si cumple de manera eficiente y con valor agregado los requerimientos de las Normas ISO/IEC 27001 :2013 y los procedimientos internos del SGSI.

- No Conformidad Mayor: Si no satisface los requerimientos de las Normas ISO27001 ; y no cumple los procedimientos internos del SGSI

- No Conformidad Menor: Si existe una desviación parcial de los requerimientos las Normas ISO/IEC 27001 :2013 ; o no cumple parcialmente con los procedimientos internos del SGSI.

- Observación: Si existe una potencial desviación a los requerimientos de las Normas ISO/IEC 27001 :2013 y los procedimientos internos del SGSI.

- Oportunidades de mejora: Sugerencias constructivas a un proceso que puede ser mejorado.

- Seguimiento y Evaluación de las auditorías deben ser establecidas en el procedimiento de Revisión por Dirección.

## 2.2.3 Gestión de indicadores.

1) **Objetivo.**

   Medir de manera eficiente los controles implementados, bajo criterios que integren la incidencia del SGSI en la gestión general de la organización.

2) **Desarrollo.**
   **Los indicadores propuestos los dividiremos en 3 grandes grupos.**

   - Seguridad Física.
   - Seguridad Lógica.
   - Incidencia del talento Humano.

En la siguiente tabla encontramos el detalle de los indicadores del Plan Director.

| INDICADORES PLAN DIRECTOR SGSI - EP AGUAS DE MANTA | | | | | |
|---|---|---|---|---|---|
| # | Responsable. | Dominio | Nombre del Indicador. | Fórmula. | Frecuencia. |
| 1 | Responsable data center / Técnico en sistemas. | Seg. Física | Incidentes de seguridad física atendidos. | Incidentes reportados / Incidentes atendidos. | Trimestral. |
| 2 | Responsable data center / Técnico en sistemas. | Seg. Física | Ingreso de personal no autorizado en áreas sensibles. | Total, de días / Días con novedades. | Trimestral. |
| 3 | Responsable data center / Técnico en sistemas. | Seg. Física | Ingreso de objetos no permitidos. | Intento de ingreso de objetos / Ejecución de ingreso, | Trimestral. |
| 4 | Responsable data center / Técnico en sistemas. | Seg. Física | Número de zonas sucias (información impresa) | Zonas de trabajo / Zonas de trabajo sucias. | Mensual |
| 5 | Responsable data center / Técnico en sistemas. | Seg. Física | Computadores sin atención. | Número de equipos / Equipos sin atención | Mensual |

| | | | | | |
|---|---|---|---|---|---|
| 6 | Oficial de Seguridad / Gerente de Tics. | Seguridad Lógica. | Incidentes de seguridad lógica atendidos. | Incidentes reportados / Incidentes atendidos. | Trimestral. |
| 7 | Oficial de Seguridad / Gerente de Tics. | Seguridad Lógica. | Falsos positivos. | Incidentes reales / Falsos positivos. | Trimestral. |
| 8 | Oficial de Seguridad / Gerente de Tics. | Seguridad Lógica. | Accesos no autorizados a Sistemas de Información. | Intentos de acceso / Ejecución, | Trimestral. |
| 9 | Oficial de Seguridad / Gerente de Tics. | Seguridad Lógica. | Intentos de ataques DDOS | Intentos de ataques / Ejecución de ataques. | Trimestral. |
| 10 | Oficial de Seguridad / Gerente de Tics. | Seguridad Lógica. | Privilegios de accesos innecesarios o improductivos. | Total de reglas de accesos / Acceso improductivos. | Trimestral. |
| 11 | Oficial de Seguridad / Gerente de Tics. | Seguridad Lógica. | Computadores sin protección lógica. | Total de computadores / Equipos desprotegidos. | Mensual |
| 12 | Gerente TTHH | Incidencia TTHH | Número de empleados capacitados en S.I. | Número total de empleados / Capacitados en SI | Trimestral. |
| 13 | Gerente TTHH | Incidencia TTHH | Difusión de políticas de seguridad de información. | Número total de empleados / Empleados que conozcan la política. | Trimestral. |
| 14 | Oficial de Seguridad / Gerente de Tics. | Incidencia TTHH | Solicitudes formales. | Solicitudes formales / Solicitudes atendidas informales. | Mensual |
| 15 | Oficial de Seguridad / Gerente de Tics. | Incidencia TTHH | Número de dispositivos personales conectados a la red. | Total de dispositivos / Total de dispositivos conectados a la red. | Mensual |

Tabla 6 - Indicadores SGSI EPAM.

## 2.2.4 Procedimiento Revisión por Dirección.

**1) Objetivo.**

El presente procedimiento detalla un esquema de pasos ordenados para llevar a cabo el proceso de Revisión por dirección del Sistema de Gestión de seguridad de la

información, que contiene el esquema de tratamiento de la información y sistemas informáticos inmersos en la gestión institucional.

La revisión por dirección es un requerimiento de la ISO/IEC 27001 :2013 que asegura la vigencia, conveniencia , adecuación , eficacia y mejora continua del SGSI. Por tanto apegado a esta norma este procedimiento considerará los siguientes puntos:

a) El estado de las acciones desde anteriores revisiones por la dirección;
b) Los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de seguridad de información;
c) La información sobre el comportamiento de la seguridad de información, incluidas las tendencias relativas a:

    1) No conformidades y acciones correctivas.
    2) Seguimiento y resultados de las mediciones.
    3) Resultados de auditoría.

    4) El cumplimiento de los objetivos de seguridad de la información.

d) Los comentarios provenientes de las partes interesadas;
e) Los resultados de la apreciación del riesgo y el estado del plan de tratamiento de riesgos.
f) Las oportunidades de mejora continua.

**2) Alcance.**

Este procedimiento aplica desde la planificación por intervalos de la revisión de todos los productos tecnológicos inmersos en el Sistema de gestión de Seguridad información ofertados por la Gerencia de Tecnologías de la Información, hasta la evaluación de los auditores internos y toma de acciones de mejora continua.

**3) Referencias.**

Para la elaboración de este documento se consideraron los criterios establecidos en:

- Norma ISO/IEC 27001 :2013 capítulo 9.3 - Revisión por dirección.
- Norma ISO/IEC 27002 :2013 capítulo 18.2 – Revisiones de la Seguridad de la información.

**4) Responsables**

- Presidente del directorio.
- Gerente General.
- Oficial de Seguridad.
- Gerente de Tecnología de Información y Comunicación.

**5) Desarrollo.**

**5.1. Programación de Revisión.**

El oficial de Seguridad tendrá la responsabilidad de establecer un cronograma anual de revisión del SGSI por parte de las autoridades pertinentes.

Esta tarea debe realizarse al menos una vez al año, pudiendo ser modificada esta frecuencia por demanda de las autoridades o por El estado y la importancia de los procesos o las áreas inmersas.

**6.2 Preparación de Revisión.**

La dirección debe tomar acciones previas al inicio de la revisión del SGSI, tales como:

- Revisión y Documentación exhaustiva acerca de revisiones por dirección anteriores. (en caso de existir).
- Consideraciones de cambios o consideraciones internas o externas que puedan afectar al SGSI.
- Revisión del plan y programación de revisión por dirección.
- Preparación una lista de verificación en cuanto a requisitos u observaciones preestablecidas (si lo considera necesario).

**6.3 Ejecución De La Revisión.**

La revisión por dirección no contará con tanta solemnidad como la auditoría sin embargo se debes establecer una serie de acciones las cuales serán documentadas, tales como:

- Establecimiento y revisión de conformidades.
- Propuesta para despliegue de acciones correctivas.
- Análisis del resultado de auditorías.
- Lista de verificación del cumplimiento de los objetivos del SGSI.
- Compilación de comentarios de la contraparte.
- Estado actual de los riesgos y su plan de tratamiento.
- Evaluación de los auditores.
- Seguimiento y evaluación - mejora continua.
- Análisis de la necesidad de auditoría por terceros.

## 2.2.5 Gestión de Roles y Responsabilidades:

**1) Objetivo.**

Establecer los roles y responsabilidades de los actores inmersos en la concepción, gestión y despliegue del SGSI.

**2) Responsables.**

La máxima autoridad o su designado tendrá el encargo de establecer los roles y designar los empleados responsables de asumir los mismo.

**3) Desarrollo.**

A continuación se detallan los roles y responsabilidades pertinentes:

**Alta directiva:** Designación otorgada a la máxima autoridad o su delegado. Puede tratarse de una persona o un equipo que fungirá como comité y tendrá como misión principal velar por el cumplimiento de la política de seguridad de la información, el SGSI en todas sus fases y comandará la revisión por dirección. Entre otras tareas se encargará de:

- Aprobar la política de seguridad y de autorizar sus modificaciones.
- Promover la difusión de este Plan director y de toda la normativa concerniente al SGSI.
- Apoyar a la seguridad de la información dentro de la organización
- Nombrar al Oficial de Seguridad.

**Oficial de Seguridad (OSI):** Es el principal responsable del SGSI, y será el encargado de articular todas las acciones que incurren en torno a la implementación y mantenimiento del Plan director de Seguridad de la información. Entre otras atribuciones y responsabilidades podrá:

- Coordinar la dirección de las actividades del SGSI.
- Determinar los niveles de seguridad de los productos tecnológicos.
- Notificar la presente política a todo el personal, e informar de los cambios que en ella se produzcan.
- Velar por la suscripción de los Acuerdos de Confidencialidad.
- Impulsar capacitación continua en materia de seguridad.
- Clasificar la información de acuerdo con el grado de criticidad.
- Notificará a todo el personal de nuevo ingreso las obligaciones respecto a la Política de Seguridad de la Información y de toda la normativa anexa.
- Elaborará los planes de auditoría y revisión por dirección.
- Elaborará plan de contingencia y recuperación de desastres.

**Auditor interno:** funcionario encargado de ejecutar las auditorías programadas según el cronograma y el plan de auditorías. Un miembro del equipo auditor será designado como auditor líder.

Entre las funciones concernientes al rol están:

- Cumplir con el despliegue de pruebas y monitoreo del SGSI.
- Informar no conformidades.
- Solicitar auditorias de terceras partes.

- Levantar informes sobre incidentes de seguridad que sobrepasen la criticidad media.
- Auditar recurrentemente los controles implementados de manera aleatoria.

**Técnico de sistemas:** Este rol puede ser designado a varios funcionarios , regularmente pertenecientes a la Gerencia de Tics, ellos serán los encargados de velar en primera línea por el cumplimiento de los controles establecidos en el SGSI como aplicables.

Entre las funciones concernientes al rol están:

- Establecer consideraciones de seguridad de información en cada ámbito del despliegue tecnológico.
- Informar sobre incidentes de seguridad.
- Levantar informes de implementación de soluciones.
- Asesorar a la alta directiva y al OSI acerca de aplicabilidad de nuevos controles.
- Capacitar en temas de Seguridad de la Información a todo el personal de la organización.
- Cumplir y hacer cumplir la política de Seguridad de la información y sus normas anexas.

### 2.2.6 Metodología de Análisis de Riesgos:

**1) Objetivo.**

Definir la metodología de análisis de riesgo, las métricas a utilizar, las responsabilidades y los procedimientos involucrados en el análisis y gestión de los riesgos de la Empresa Pública Aguas de Manta, con la finalidad de proporcionar una guía sencilla y de rápida aplicación para la identificación y análisis de riesgos, y así obtener un insumo final para el tratamiento de riesgos.

La metodología elegida debe estar enmarcada en evaluar las 3 principales aristas de Seguridad de Información, tales como Confidencialidad, Integridad y Disponibilidad, regularmente el riesgo necesita ser detectado y tratado usando métricas que permitan la aproximación inmediata para resolverlo o neutralizarlo.

**2) Responsables.**

La definición de la metodología para el análisis de riesgo será definida por los miembros de la Alta Directiva (comité de seguridad) y podrá ser modificada bajo sustentos técnicos o circunstancias especiales.

**3) Desarrollo.**

La metodología elegida para el despliegue de este Plan Director es MAGERIT versión 3.0, un esquema idóneo para aquellas empresas que están iniciando con la gestión de la seguridad de la información, pues enfoca sus esfuerzos en canalizar los riesgos que tienen mayor incidencia para el despliegue informático de la organización. Se trata de una metodología ampliamente reconocida.

Una de las bondades de MAGERIT v3.0 es que expone sus resultados de manera cuantitativa, en porcentajes de riesgos y valores económicos, lo que convierte su producto final en un insumo fácil de consumir para los tomadores de decisiones.

MAGERIT v3.0 se basa en buscar e identificar las amenazas que pueden afectar a la gestión de la seguridad y el impacto que estas puedan tener en diferentes niveles para la organización , por lo cual su empleo es sumamente vital a la hora identificar medidas preventivas y correctivas para tratar y minimizar los riesgos previamente analizados.
En síntesis MAGERIT v3.0 consta de varias fases tales como:

1. Identificar los activos relevantes para la Organización, su relación y su valor, en el contexto de las pérdidas que supondría su degradación.
2. Determinar a qué amenazas están expuestos los activos previamente identificados.
3. Establecer salvaguardas y su consecusión frente al riesgo asociado.
4. Estimar el impacto, en virtud del daño sobre el activo derivado en caso de la materialización de la amenaza.
5. Evaluar el riesgo, orientado su incidencia como el impacto ponderado con el nivel de fecuencia de la amenaza.

En detalle las fases previamente numeradas:

**Identificación de activos:** Etapa inicial donde es necesario realizar una identificación y valorar los activos transcendentales involucrados en el ámbito de seguridad de la información, estos activos identificados serán los elementos por proteger.
Los activos serán clasificados según el catálogo de elementos anexo en el libro II de Magerit V3.0, donde encontramos las siguientes divisiones según su especie.

- Activos esenciales.- Marcan requisitos de confidencialidad.
- Arquitectura del sistema.- permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior.
- Datos/ Información.- Ficheros, activos transcendentales de la organización.
- Claves criptográficas.- Certificados de claves públicas o privadas.
- Servicios.- Servicios informaticos orientados a necesidades de usuarios.
- Software.- Activos intangibles de programas propietario o de desarrollo propio.
- Equipamiento informático (hardware).- Materiales, físicos, destinados a soportar directa o indirectamente los servicios informáticos.
- Redes de comunicaciones.- Activos concernientes a comunicación de datos.
- Soportes de información.- Soportes de medios electrónicos para almacenamiento o respaldo de información.
- Equipamiento Auxiliar.- Activos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
- Innstalaciones.
- Personal.- Contingente humano involucrado en la gestión organizacional.

**Valoración de los activos:** Para fines de cálculos y aplicación metodológica es necesario que los activos cuenten con una valoración.
Las dimensiones de valoración se determinan conforme a las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión se expone en virtud del perjuicio para la organización si el activo resulta afectado según ese

criterio. Estas dimensiones vienen establecidas por las aristas principales de seguridad de información.

**[D] disponibilidad.-** Concepto que define la capacidad de los activos que tienen acceso a los servicios u otros activos cuando lo requieren.
¿Qué importancia tendría que el activo no estuviera disponible?
Este criterio debe ser medido en según la valoración desde el punto de vista de disponibilidad si una amenaza afectara a su disponibilidad, evaluando las consecuencias que existieran de materializarse el impacto.
Lateralmente existe una contra postura para la valoración de un activo que carece de un valor no apreciable desde el punto de vista de disponibilidad cuando su funcionamiento puede estar ausente durante largos periodos de tiempo o de manera repetitiva sin que su impacto sea significativo para la organización. En este concepto se establece que la disponibilidad es una característica que afecta a todo tipo de activos.

**[I] integridad.-** Consiste en la cualidad en la aquel activo no ha sufrido cambios de manera ilegal , forzosa o no autorizada.
¿Qué importancia tendría que los datos fueran modificados arbitrariamente?
El tipo de activos "datos" recibe una significante valoración de integridad cuando su modificación o alteración no consentida repercute de manera graves a la organización, asimismo volvemos a la analogía de que si la no integridad de ciertos datos no afecta en nada a la organización su valoración en este rubro sería nula.

**[C] confidencialidad.-**
Criterio que tiene como premisa que la información no se difunde ni se entrega a entidades no autorizadas (entiéndase por entes a personas, procesos, organizaciones externas, autoridades).
¿Qué incidencia tendría que la información fuera conocido por personas ajenas a su naturaleza?
Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando conocimiento su revelación pública o no autorizada deriva en graves daños para la entidad. Los datos que no poseen calificación notable respecto a confidencialidad cuando su conocimiento por cualquiera no supone riesgo latente.

Para el fin de esta implantación y por la naturaleza de la organización es recomendable establecer una escala económica para su estimación monetaria según su costo , y otro campo que contenga el criterio de su incidencia en el correcto curso de las operaciones de la organización, tal como lo vemos en el libro III, cap.4 de MAGERIT V3.0.

El criterio mencionado anteriormente lo vemos plasmados en las dos siguientes tablas.

| VALORACIÓN DE LOS ACTIVOS SEGÚN INCIDENCIA. | | |
|---|---|---|
| **NIVEL** | **RANGO** | **DEFINICIÓN** |
| Muy alto (MA) | MAYOR A 100 MIL $ USD | La pérdida o indisponibilidad del activo resultaría catastrófico para la compañía. |
| Alto (A) | MAYOR A 30 MIL $ MENOR A 100 MIL $ | La pérdida o indisponibilidad del activo afecta considerablemente a la compañía. |
| Medio (M) | MAYOR A 5 MIL $ MENOR A 30 MIL $ | La pérdida o indisponibilidad del activo afecta levemente a la compañía. |

| | | |
|---|---|---|
| Bajo (B) | MAYOR A 1 MIL $ MENOR A 5 MIL $ | La pérdida o indisponibilidad del activo afecta imperceptiblemente a la compañía. |
| Muy bajo (MB) | MENOR A 1 MIL $ USD | La pérdida o indisponibilidad del activo apenas afecta a la compañía . |

*Tabla 7 - Valoración Económica de Activos.*

Para la valoración cualitativa según la gravedad del daño de los activos según su incidencia se establece un rango de valores según el criterio, esta calificación se medirá evaluando las principales aristas de seguridad de la información: Confiabilidad, Integridad y Disponibilidad.

| VALOR | | CRITERIO |
|---|---|---|
| 10 | EXTREMO | Daño extremadamente grave. |
| 9 | MUY ALTO | Daño muy grave |
| (6-8) | ALTO | Daño grave |
| (3-5) | MEDIO | Daño importante |
| (1-2) | BAJO | Daño menor |
| 0 | DESPRECIABLE | Irrelevante |

*Tabla 8 - Valoración Cualitativa Activos.*

**Identificación de amenazas:** En esta etapa es procedente identificar y valorar las amenazas a las que se encuentran expuestos los activos previamente identificados.
El catálogo de amenazas se aplica según la afectación que surjan en caso de su materialización a la Confiabilidad, Integridad y Disponibilidad de la información.
Las amenazas según su tipo pueden afectar una, dos o tres de estas aristas, eso ha sido definido por la ficha de cada tipo de activos especificado en el catálogo de elementos, Libro II cap.5 MAGERIT v3.0, en este catálogo encontramos clasificaciones y subclases de amenazas que son enmarcadas por el tipo de activo vs la dimensión.

Las principales clases de amenazas son:

**1. [N] Desastres naturales.-** Incidentes cuya ocurrencia no tienen responsabilidad humana directa ni indirecta. Ejemplo: Fuego, Huracanes, terremotos, etc.
Afecta regularmente a la disponibilidad de los activos.

**2. [I] De origen industrial.-** Amenazas ocurrentes de forma accidental mediante la intervención humana de tipo industrial, ya sea de forma aleatoria o intencionada. Ejemplo: Incendio, Desastres industriales, sobrecarga eléctrica, accidentes de tráfico, etc.

**3. [E] Errores y fallos no intencionados.-** Errores no intencionales provocados por personal humano. Ejemplo: errores de usuarios, borrado accidental de información , errores administrativos, errores de configuración, etc.
Este apartado puede afectar a los 3 rubros, Confidencialidad, Integridad y Disponibilidad.

**4. [A] Ataques intencionados.-** Errores intencionales y premeditados provocados por personal humano. Ejemplo: manipulación de registros, alteración de la configuración, uso no previsto, abuso de privilegios.

Este apartado afecta a los 3 rubros, Confidencialidad, Integridad y Disponibilidad.

**5. Correlación de errores y ataques.-** Errores que tienen características de las dos especies recién abordadas, combinando variantes de tal manera que pueden resultar en:

- Amenazas que sólo pueden ser errores, nunca ataques deliberados.
- Amenazas que nunca son errores: siempre son ataques deliberados.
- Amenazas que pueden producirse tanto por error como deliberadamente.

La frecuencia con la que se pronóstica para las amenazas latentes en virtud de cada activo es reflejada en la siguiente tabla, la unidad mínima de frecuencia será diaria y la máxima anual.
Esta valoración frecuencial va acompañada de un valor numérico que es expresado desde 100 a 0.01 , donde 100 valora las amenazas cuya ocurrencia es muy elevada, y donde 0.01 califica las amenazas con ocurrencia menor a una vez al año.

| FRECUENCIA | RANGO | VALOR |
|---|---|---|
| Frecuencia muy alta (FMA) | Una vez al día | 100 |
| Frecuencia alta (FA) | Una vez al mes | 10 |
| Frecuencia media (FM) | Una vez cada trimestre | 1 |
| Frecuencia baja (FB) | Una vez cada semestre | 0.1 |
| Frecuencia muy baja (FMB) | Una vez al año | 0.01 |

*Tabla 9 - Frecuencia amenazas.*

En la tabla de ejemplo que acontinuación se presenta podemos observar el tipo de activo, el detalle del activo, la frecuencia según el impacto y el listado de amenazas y el porcentaje de afectación a la Confiabilidad, Integridad y Disponibilidad. El valor del porcentaje de impacto por cada activo será el promedio del impacto de las amenazas que lo involucran.

Cada activo contará con un porcentaje de impacto por cada cada criterio de seguridad de información, donde C = Confidencialidad , I= Integridad , D= Disponibilidad.

| TIPO DE ACTIVO | | | | |
|---|---|---|---|---|
| **NOMBRE DE ACTIVO** | | **%** | **%** | **%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| Amenaza 1 | FMA | % | % | % |
| Amenaza 2 | FA | % | % | % |
| Amenaza 3 | FM | % | % | % |
| Amenaza N…. | FB | % | % | % |

*Tabla 10 - Identificación de Amenazas.*

**Cálculo del impacto Potencial:** En este paso se calculará el impacto, que resulta de la formula donde se define el valor del activo multiplicado por el daños que se puede producir sobre el activo al producirse la amenaza. Este cálculo resulta en la cuantificación del daño del activo involucrado.

**Impacto = Valor del activo (criticidad) x Porcentaje de impacto**

Cada activo contará con un porcentaje de impacto por cada cada criterio de seguridad de información, donde C = Confidencialidad , I= Integridad , D= Disponibilidad.

| ÁMBITO | ACTIVO | CRITICIDAD | | | %IMPACTO | | | IMPACTO POTENCIAL | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | C | I | D | C | I | D | C | I | D |
| **Tipo de activo** | Activo 1 | C | I | D | % | % | % | **C*%** | **I*%** | **D*%** |
| | Activo N…. | C | I | D | % | % | % | **C*%** | **I*%** | **D*%** |

*Tabla 11 - Cálculo Impacto Potencial.*

**Cálculo del riesgo potencial:** Una vez que se ha calculado el impacto potencial se puede calcular el riesgo potencial asociado teniendo en cuenta la frecuencia con la que puede tener lugar la amenaza.
El valor numérico de la frecuencia estará dado por la cuantificación definida en la tabla 9 – Frecuencia de amenazas, incluida en el presente documento.

El impacto potencial ya no se encontrará en porcentaje sino en cantidades enteras con dos decimales, para facilitar el cálculo matemático.

**Riesgo = Frecuencia x Impacto**

Cada activo contará con una calificación de riesgo por cada cada criterio de seguridad de información, donde C = Confidencialidad , I= Integridad , D= Disponibilidad.

| ÁMBITO | ACTIVO | FRECUENCIA | | IMPACTO POTENCIAL | | | RIESGO POTENCIAL | | |
|---|---|---|---|---|---|---|---|---|---|
| | | FREC | VAL | C | I | D | C | I | D |
| **Hardware [HW]** | AACC de precisión. | **FMA** | **100** | C | I | D | **C*VAL** | **I*VAL** | **D*VAL** |
| | Cableado estructurado. | **FA** | **10** | C | I | D | **C*VAL** | **I*VAL** | **D*VAL** |
| | CCTV (video vigilancia). | **FB** | **1** | C | I | D | **C*VAL** | **I*VAL** | **D*VAL** |

*Tabla 12 - Modelo para el cálculo del riesgo potencial.*

**Definición del umbral del riesgo:** El riesgo puntuará según un rango que tendrá que ser definido por los involucrados en la seguridad de la información de la organización, para efectos de este documento el riesgo aceptable puntuará por debajo de los 40 puntos.

Los activos que obtengan una puntuación mayor o igual a 40 serán catalogados como activos con un nivel de riesgo no aceptable y tendrán que ser tratados de manera inmediata con la definición de proyectos.

### 2.2.7 Declaración de aplicabilidad:

1) **Objetivo.**

Definir los controles del Anexo A de la ISO/IEC 27001 :2013 con el propósito de indicar la aplicabilidad de estos en la Empresa Pública Aguas de Manta.

2) **Responsables.**
   - Alta Directiva.
   - Oficial de Seguridad.
   - Técnico de sistemas. (Asesor).

**3) Desarrollo.**

| CONTROL | | | | APLICABILIDAD | JUSTIFICACIÓN |
|---|---|---|---|---|---|
| A.5 Information security policies | | | | | |
| | A.5.1 Management direction for information security | | | | |
| | | A.5.1.1 | Policies for information security | SI | Debe existir este documento habilitante con la finalidad de establecer normas de SI. |
| | | A.5.1.2 | Review of the policies for information security | SI | Debe existir una revisión periódica de este rubro. |
| A.6 Organization of information security | | | | | |
| | A.6.1 Internal organization | | | | |
| | | A.6.1.1 | Information security roles and responsibilities | SI | Aplica ya que es necesario contar con un marco de roles y responsabilidades. |
| | | A.6.1.2 | Segregation of duties | | |
| | | A.6.1.3 | Contact with authorities | SI | Aplica debido a que se trata de una organización gubernamental. |
| | | A.6.1.4 | Contact with special interest groups | SI | Aplica porque que la organización debe mantenerse actualizada y asesorada constantemente. |
| | | A.6.1.5 | Information security in project management | SI | La gestión de proyectos debe seguir un flujo que considere las repercusiones de no contar con seguridad de la información. |
| | A.6.2 Mobile devices and teleworking | | | | |
| | | A.6.2.1 | Mobile device policy | SI | La organización debe aplicar este control como indispensable. |
| | | A.6.2.2 | Teleworking | SI | La organización ha adoptado el Teletrabajo como una alternativa y deben existir normas y procedimientos documentados sobre su correcto uso y el tratamiento de la información. |

| | | | | | |
|---|---|---|---|---|---|
| A.7 Human resource security | | | | | |
| | A.7.1 Prior to employment | | | | |
| | | A.7.1.1 | Screening | SI | Al manejarse información de alta criticidad y dominio es necesario establecer este requisito. |
| | | A.7.1.2 | Terms and conditions of employment | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica |
| | A.7.2 During employment | | | | |
| | | A.7.2.1 | Management responsibilities | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica. |
| | | A.7.2.2 | Information security awareness, education, and training | | |
| | | A.7.2.3 | Disciplinary process | | |
| | A.7.3 Termination and change of employment | | | | |
| | | A.7.3.1 | Termination or change of employment responsibilities | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica |
| A.8 Asset management | | | | | |
| | A.8.1 Responsibility for asset | | | | |
| | | A.8.1.1 | Inventory of assets | SI | Es importante definir responsabilidades de protección adecuadas para los activos. |
| | | A.8.1.2 | Ownership of assets | SI | Es importante definir responsabilidades de protección adecuadas para los activos. |
| | | A.8.1.3 | Acceptable use of assets | SI | Es importante definir responsabilidades de protección adecuadas para los activos. |
| | | A.8.1.4 | Return of assets | SI | Es importante definir responsabilidades de protección adecuadas para los activos. |
| | A.8.2 Information classification | | | | |
| | | A.8.2.1 | Classification of information | SI | Es indispensable el etiquetado y clasificación de información para la organización. |
| | | A.8.2.2 | Labelling of Informa tion | | |

| | | | | | |
|---|---|---|---|---|---|
| | | A.8.2.3 | Handling of assets | SI | La información en su gran mayoría es tratada y modificada para su gestión. |
| | A.8.3 Media handling | | | | |
| | | A.8.3.1 | Management of removable media | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica |
| | | A.8.3.2 | Disposal of media | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica |
| | | A.8.3.3 | Physical media transfer | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica |
| A.9 Access control | | | | | |
| | A.9.1 Business requirements of access control | | | | |
| | | A.9.1.1 | Access control policy | SI | Aplica debido a que se trata de una organización gubernamental. |
| | | A.9.1.2 | Access to networks and network services | SI | Aplica debido a que se trata de una organización gubernamental. |
| | A.9.2 User access management | | | | |
| | | A.9.2.1 | User registration and de-registration | SI | Aplica debido a que se trata de una organización gubernamental. |
| | | A.9.2.2 | User access provisioning | SI | Aplica debido a que se trata de una organización gubernamental. |
| | | A.9.2.3 | Management of privileged access rights | SI | Aplica debido a que se trata de una organización gubernamental. |
| | | A.9.2.4 | Management of secret authentication information of users | SI | Aplica debido a que se trata de una organización gubernamental. |
| | | A.9.2.5 | Review of user access rights | SI | Aplica debido a que se trata de una organización gubernamental. |
| | | A.9.2.6 | Removal or adjustment of access rights | SI | Aplica debido a que se trata de una organización gubernamental. |
| | A.9.3 User responsibilities | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | A.9.3.1 | Use of secret authentication information | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica |
| | A.9.4 System and application access control | | | | |
| | | A.9.4.1 | Information access restriction | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica |
| | | A.9.4.2 | Secure log-on procedures | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica |
| | | A.9.4.3 | Password management system | SI | Aplica debido a que los usuarios finales manejan información crítica día a día. |
| | | A.9.4.4 | Use of privileged utility programs | SI | Aplica para evitar daños permanentes en sistemas y BD. |
| | | A.9.4.5 | Access control to program source code | SI | Aplica para evitar daños permanentes en sistemas y BD. |
| A.10 Cryptography | | | | | |
| | A.10.1 Cryptographic controls | | | | |
| | | A.10.1.1 | Policy on the use of cryptographic controls | SI | Aplicación sumamente necesaria para proteger la información de amenazas maliciosas. |
| | | A.10.1.2 | Key management | SI | Aplicación sumamente necesaria para proteger la información de amenazas maliciosas. |
| A.11 Physical and environmental security | | | | | |
| | A.11.1 Secure areas | | | | |
| | | A.11.1.1 | Physical security perimeter | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica |
| | | A.11.1.2 | Physical entry controls | SI | Aplica, para mantener los parámetros de seguridad física en las áreas de centro de datos. |

| | | | | | |
|---|---|---|---|---|---|
| | | A.11.1.3 | Securing offices, rooms, and facilities | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica |
| | | A.11.1.4 | Protecting against external and environmental threats | SI | Es imprescindible contar con un plan de contingencia y recuperación de desastres. |
| | | A.11.1.5 | Working in secure areas | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica |
| | | A.11.1.6 | Delivery and loading areas | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica |
| | A.11.2 Equipment | | | | |
| | | A.11.2.1 | Equipment siting and protection | SI | Es necesario contar con este control para evitar daños irreversibles en estaciones de trabajo. |
| | | A.11.2.2 | Supporting utilities | SI | Es necesario contar con este control para evitar daños irreversibles en estaciones de trabajo. |
| | | A.11.2.3 | Cabling security | SI | Es necesario contar con este control para evitar daños irreversibles en estaciones de trabajo. |
| | | A.11.2.4 | Equipment maintenance | SI | Es necesario contar con este control para evitar daños irreversibles en estaciones de trabajo. |
| | | A.11.2.5 | Removal of assets | SI | Aplica como medida de seguridad de los usuarios finales. |
| | | A.11.2.6 | Security of equipment and assets off-premises | SI | Aplica como medida de seguridad de los usuarios finales. |
| | | A.11.2.7 | Secure disposal or reuse of equipment | SI | Aplica como medida de seguridad de los usuarios finales. |
| | | A.11.2.8 | Unattended user equipment | SI | Aplica como medida de seguridad de los usuarios finales. |
| | | A.11.2.9 | Clear desk and clear screen policy | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica |
| A.12 Operations security | | | | | |

| | | | | |
|---|---|---|---|---|
| A.12.1 Operational procedures and responsibilities | | | | |
| | A.12.1.1 | Documented operating procedures | SI | Aplica debido a que se trata de una organización gubernamental. |
| | A.12.1.2 | Change management | SI | Aplica debido a que se trata de una organización gubernamental. |
| | A.12.1.3 | Capacity management | SI | Aplica debido a que se trata de una organización gubernamental. |
| | A.12.1.4 | Separation of development, testing and operational environments | SI | Aplica para evitar daños permanentes en sistemas y BD. |
| A.12.2 Protection from malware | | | | |
| | A.12.2.1 | Controls against malware | SI | Aplicación sumamente necesaria para proteger la información de amenazas maliciosas. |
| A.12.3 Backup | | | | |
| | A.12.3.1 | Information backup | SI | Aplica debido a que se trata de una organización gubernamental. |
| A.12.4 Logging and monitoring | | | | |
| | A.12.4.1 | Event logging | SI | Aplicación sumamente necesaria para la ejecución de auditorías. |
| | A.12.4.2 | Protection of log information | SI | Aplicación sumamente necesaria para la ejecución de auditorías. |
| | A.12.4.3 | Administrator and operator logs | SI | Aplicación sumamente necesaria para la ejecución de auditorías. |
| | A.12.4.4 | Clock synchronisation | SI | Aplicación sumamente necesaria para la ejecución de auditorías. |
| A.12.5 Control of operational software | | | | |
| | A.12.5.1 | Installation of software on operational systems | SI | Aplica para evitar daños permanentes en sistemas y BD. |
| A.12.6 Technical vulnerability management | | | | |
| | A.12.6.1 | Management of technical vulnerabilities | SI | Aplicación sumamente necesaria para proteger la información de amenazas maliciosas. |
| | A.12.6.2 | Restrictions on software installation | SI | Aplicación sumamente necesaria para proteger la información de amenazas maliciosas. |

| | | | | | |
|---|---|---|---|---|---|
| | A.12.7 Information systems audit considerations | | | | |
| | | A.12.7.1 | Information systems audit controls | SI | Aplicación sumamente necesaria para la ejecución de auditorías. |
| A.13 Communications security | | | | | |
| | A.13.1 Network security management | | | | |
| | | A.13.1.1 | Network controls | SI | Aplica para la gestión y control de información que viaja por las redes de datos. |
| | | A.13.1.2 | Security of network services | SI | Aplica para la gestión y control de información que viaja por las redes de datos. |
| | | A.13.1.3 | Segregation in networks | SI | Aplica para la gestión y control de información que viaja por las redes de datos. |
| | A.13.2 Information transfer | | | | |
| | | A.13.2.1 | Information transfer policies and procedures | SI | Aplica efectivamente ya que existe mucha fuga de información. |
| | | A.13.2.2 | Agreements on information transfer | SI | Aplica efectivamente ya que existe mucha fuga de información. |
| | | A.13.2.3 | Electronic messaging | SI | Aplica efectivamente ya que existe mucha fuga de información. |
| | | A.13.2.4 | Confidentiality or nondisclosure agreements | SI | Aplica efectivamente ya que existe mucha fuga de información. |
| A.14 System acquisition, development, and maintenance | | | | | |
| | A.14.1 Security requirements of information systems | | | | |
| | | A.14.1.1 | Information security requirements analysis and specification | SI | Aplica debido a que se trata de una organización gubernamental. |
| | | A.14.1.2 | Securing application services on public networks | SI | Aplica debido a que se trata de una organización gubernamental. |
| | | A.14.1.3 | Protecting application services transactions | SI | Aplica debido a que se trata de una organización gubernamental. |
| | A.14.2 Security in development and support processes | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | A.14.2.1 | Secure development policy | SI | Aplica para evitar daños permanentes en sistemas y BD. |
| | | A.14.2.2 | System changes control procedures. | SI | Aplica para evitar daños permanentes en sistemas y BD. |
| | | A.14.2.3 | Technical review of applications after operating platform | SI | Aplica para evitar daños permanentes en sistemas y BD. |
| | | A.14.2.4 | Restrictions on changes to software packages | SI | Aplica para evitar daños permanentes en sistemas y BD. |
| | | A.14.2.5 | Secure system engine nearing principles | SI | Aplica para ejecución de auditorías. |
| | | A.14.2.6 | Secure development environment | SI | Aplica para evitar daños permanentes en sistemas y BD. |
| | | A.14.2.7 | Outsourced development | SI | Aplica debido a que se trata de una organización gubernamental. |
| | | A.14.2.8 | System security testing | SI | Aplica para evitar daños permanentes en sistemas y BD. |
| | | A.14.2.9 | System acceptance testing | SI | Aplica para evitar daños permanentes en sistemas y BD. |
| | A.14.3 Test data | | | | |
| | | A.14.3.1 | Protection of test data | SI | Aplica para evitar daños permanentes en sistemas y BD. |
| A.15 Supplier relationships | | | | | |
| | A.15.1 Information security in supplier relationships | | | | |
| | | A.15.1.1 | Information security policy for supplier relationships | SI | Aplica porque que la organización debe mantenerse actualizada y asesorada constantemente. |
| | | A.15.1.2 | Addressing security within supplier agreements | SI | Aplica porque que la organización debe mantenerse actualizada y asesorada constantemente. |
| | | A.15.1.3 | Information and communication technology supply chain | SI | Aplica porque que la organización debe mantenerse actualizada y asesorada constantemente. |
| | A.15.2 Supplier service delivery management | | | | |
| | | A.15.2.1 | Monitoring and review of supplier services | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica |

| | | | | | |
|---|---|---|---|---|---|
| | | A.15.2.2 | Managing changes to supplier services | SI | Es necesaria la aplicabilidad de este control debido a que muchos actores y terceros tienen a su disposición información altamente crítica |
| A.16 Information security incident management | | | | | |
| | A.16.1 Management of information security incidents and improvements | | | | |
| | | A.16.1.1 | Responsibilities and procedures | SI | Control de aplicabilidad necesaria para la gestión de incidentes. |
| | | A.16.1.2 | Reporting information security events | SI | Control de aplicabilidad necesaria para la gestión de incidentes. |
| | | A.16.1.3 | Reporting information security weaknesses | SI | Control de aplicabilidad necesaria para la gestión de incidentes. |
| | | A.16.1.4 | Assessment of and decision on information security events | SI | Control de aplicabilidad necesaria para la gestión de incidentes. |
| | | A.16.1.5 | Response to information security incidents | SI | Control de aplicabilidad necesaria para la gestión de incidentes. |
| | | A.16.1.6 | Learning from information security incidents | SI | Control de aplicabilidad necesaria para la gestión de incidentes. |
| | | A.16.1.7 | Collection of evidence | SI | Control de aplicabilidad necesaria para la gestión de incidentes. |
| A.17 Information security aspects of business continuity management | | | | | |
| | A.17.1 Information security continuity | | | | |
| | | A.17.1.1 | Planning information security continuity | SI | Aplica tajantemente para asegurar la continuidad de las operaciones. |
| | | A.17.1.2 | Implementing information security continuity | SI | Aplica tajantemente para asegurar la continuidad de las operaciones. |
| | | A.17.1.3 | Verify, review, and evaluate information security continuity | SI | Aplica tajantemente para asegurar la continuidad de las operaciones. |
| | A.17.2 Redundancies | | | | |
| | | A.17.2.1 | Availability of information processing facilities | SI | Aplica tajantemente para asegurar la continuidad de las operaciones. |
| A.18 Compliance | | | | | |
| | A.18.1 Compliance with legal and contractual requirements | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | A.18.1.1 | Identification of applicable legislation and contractual requirements | SI | Aplica para dar cumplimiento a la normativa y planes desplegados. |
| | | A.18.1.2 | Electoral property rights | SI | Aplica para dar cumplimiento a la normativa y planes desplegados. |
| | | A.18.1.3 | Protection of records | SI | Aplica para dar cumplimiento a la normativa y planes desplegados. |
| | | A.18.1.4 | Privacy and protection of personally identifiable information | SI | Aplica para dar cumplimiento a la normativa y planes desplegados. |
| | | A.18.1.5 | Regulation of cryptographic controls | SI | Aplica para dar cumplimiento a la normativa y planes desplegados. |
| | A.18.2 Information security reviews | | | | |
| | | A.18.2.1 | Independent review of information security | SI | Aplica para garantizar el funcionamiento eficiente del SGSI |
| | | A.18.2.2 | Compliance with security policies and standards | SI | Aplica para garantizar el funcionamiento eficiente del SGSI |
| | | A.18.2.3 | Technical compliance review | SI | Aplica para garantizar el funcionamiento eficiente del SGSI |

*Tabla 13 - GAP declaración de aplicabilidad*

# 3. Análisis de riesgos.

## 3.1 Introducción.

El análisis de riesgo es el elemento fundamental del plan director de Seguridad de la información, puesto que nos dará como insumo final un panorama de los riesgos a tratar y las medidas que deben ser tomadas para garantizar la seguridad de nuestros activos (infraestructura tecnológica).

Esta Fase resulta esencial en el proceso de despliegue de cualquier modelo de gestión de Seguridad de la Información, su estrecha relación con los objetivos que persigue la organización la hacen un elemento estratégico, ya que el análisis decide el rumbo de la gestión de riesgos, al definir los activos ,procesos, brechas y dominios involucrados en la Seguridad de la Información.

Luego de definir la metodología para el análisis y la clasificación de los riesgos procedemos al levantamiento de un inventario de activos, los cuales serán evaluados con la intención de protegerlos y calcular su impacto en caso de indisponibilidad. Una vez realizada esta tarea es imprescindible Identificar las amenazas y vulnerabilidades de los activos para lograr establecer el cálculo del valor de riesgo asociado a cada activo.

## 3.2 Inventario De Activos.

La identificación de activos propensos a riesgos es el primer paso para iniciar nuestro análisis. MAGERIT en su tercer libro, capitulo 2.1 nos presenta la estimación cualitativa de los activos, donde cada escala es útil para calificar la magnitud del impacto y el riesgo asociado dando como resultado un valor cuantitativo , tomando en cuenta la premisa que el costo de las medidas de seguridad no debe superar el costo del activo protegido.

El valor de cada activo se expresa en la escala de Alto, Medio y Bajo; pero se propone también para fines metodológicos valorar la incidencia bajo las tres aristas de la Seguridad de la Información (Confidencialidad , Integridad y Disponibilidad), puntuando en una escala del 1 al 10 la repercusión que tendría para cada pilar si el activo sufriera un daño o si resulta afectado por alguna amenaza.

| ÁMBITO | ACTIVO | VALOR | C | I | D |
|---|---|---|---|---|---|
| **Hardware [HW]** | AACC de precisión. | Alto | 4 | 8 | 10 |
| | Cableado estructurado. | Alto | 8 | 8 | 8 |
| | CCTV (video vigilancia). | Medio | 8 | 8 | 8 |
| | Dispositivos biométricos. (Acceso y Asistencia) | Muy bajo | 8 | 6 | 8 |
| | Dispositivos telefónicos. | Bajo | 6 | 6 | 8 |
| | Equipos de red. (ACCESS POINT, SWITCH) | Alto | 10 | 10 | 8 |
| | Estaciones de trabajo. | Alto | 6 | 6 | 6 |
| | Firewalls. | Alto | 10 | 8 | 10 |
| | Impresoras. | Bajo | 4 | 2 | 4 |
| | Routers. | Alto | 6 | 6 | 10 |
| | Servidor de archivos. (NAS) | Alto | 8 | 6 | 8 |

| | | | | | |
|---|---|---|---|---|---|
| | Servidor de correo electrónico. | Alto | 8 | 6 | 8 |
| | Servidor de telefonía IP. | Medio | 2 | 8 | 10 |
| | Servidor Georreferenciación. (GIS) | Medio | 8 | 6 | 8 |
| | Servidores de autómatas (SCADA). | Alto | 10 | 8 | 10 |
| | Servidores de virtualización. | Alto | 10 | 8 | 10 |
| | UPS | Medio | 4 | 8 | 10 |
| Software [SW] | Antivirus. | Alto | 8 | 8 | 8 |
| | Aplicaciones internas. | Alto | 8 | 8 | 10 |
| | Herramientas de desarrollo . | Bajo | 8 | 10 | 4 |
| | Programas utilitarios. | Medio | 2 | 2 | 2 |
| | Sistemas operativos. | Bajo | 4 | 4 | 6 |
| | Software de Correo electrónico. | Alto | 10 | 6 | 8 |
| | Software de virtualización. | Medio | 6 | 8 | 10 |
| | Software SCADA. | Alto | 6 | 8 | 10 |
| PERSONAL [P] | Alta Gerencia (Toma de decisiones). | Alto | 2 | 8 | 8 |
| | Control de Accesos. (Guardianía) | Bajo | 2 | 8 | 10 |
| | Desarrolladores de software. | Alto | 10 | 8 | 8 |
| | Personal externo. (proveedores, contratistas). | Medio | 2 | 8 | 6 |
| | Personal operativo (personal obrero/limpieza). | Alto | 2 | 2 | 2 |
| | Personal tecnológico (infraestructura - soporte). | Alto | 10 | 8 | 8 |
| | Usuarios finales. (personal administrativo). | Alto | 10 | 8 | 8 |
| Instalaciones [L] | Centros de Datos. | Muy alto | 2 | 8 | 10 |
| | Centro de Monitoreo (Sala de Control SCADA). | Alto | 2 | 8 | 10 |
| | Instalaciones estructurales. (Edificio, estaciones). | Muy alto | 2 | 8 | 10 |
| | Laboratorios de Agua Potable. | Alto | 2 | 6 | 6 |
| | Plantas de bombeo y tratamiento. | Alto | 2 | 8 | 6 |
| Servicios [S] | Correo electrónico. | Alto | 8 | 6 | 8 |
| | Infraestructura cloud. | Muy alto | 10 | 6 | 10 |
| | Portales tecnológicos publicados. | Medio | 10 | 6 | 10 |
| | Sitio Web institucional. | Medio | 8 | 6 | 8 |
| | SWITCH transaccionales. (intercambio electrónico de datos) | Alto | 10 | 10 | 10 |
| Datos. [D] | Datos de clientes (abonados). | Muy alto | 8 | 10 | 10 |
| | Datos de gestión interna. | Alto | 6 | 8 | 10 |
| | Datos financieros - contables. | Muy alto | 8 | 10 | 10 |
| | Información de usuarios (personal). | Bajo | 2 | 2 | 2 |
| | Registros de actividad (logs). | Medio | 8 | 8 | 10 |

*Tabla 14 - Valoración de Activos.*

## 3.3 Análisis De Amenazas.

Una vez identificados los activos, su valor cualitativo respecto al nivel de incidencia y puntuarlos respecto a los criterios de Confidencialidad, Integridad y Disponibilidad procedemos a realizar el análisis de las amenazas bajos ciertos criterios.

Siguiendo el catálogo de elementos MAGERIT en su Libro 2, capítulo 5 las amenazas se clasifican según su origen en:

- Desastres naturales.- [N] Eventos naturales que no involucran intervención humana de manera directa ni indirecta.
    - [N.1] Fuego
    - [N.2] Daños por agua
    - [N.*] Desastres naturales (Ej.: Fuego, inundaciones, Terremoto).

- De origen industrial.- [I] Sucesos accidentales consecuencia de actividades humanas ligadas a procesos mecánicos o industriales.
    - [I.1] Fuego.
    - [I.2] Daños por agua.
    - [I.3] Desastres industriales.
    - [I.4] Contaminación electromagnética.
    - [I.5] Avería de origen físico o lógico.
    - [I.6] Corte de suministro eléctrico.
    - [I.7] Condiciones inadecuadas de temperatura o humedad
    - [I.8] Fallo de servicios de comunicaciones.
    - [I.9] Interrupción de otros servicios y suministros esenciales
    - [I.10] Degradación de los soportes de almacenamiento de la información.
    - [I.11] Emanaciones electromagnéticas.

- Errores o fallos no intencionados.- [E] Amenazas de origen humano/accidental.
    - [E.1] Errores de los usuarios.
    - [E.2] Errores del administrador.
    - [E.3] Errores de monitorización.
    - [E.4] Errores de configuración.
    - [E.7] Deficiencias organizacionales.
    - [E.8] Difusión de SW dañino.
    - [E.9] Errores de [re]-encaminamiento.
    - [E.10] Errores de secuencia.
    - [E.15] Alteración accidental de la información.
    - [E.18] Destrucción de la información.
    - [E.19] Fugas de información.
    - [E.20] Vulnerabilidades de los programas (SW).

- [E.21] Errores de mantenimiento / actualización de programas.
- [E.23] Errores de mantenimiento / actualización de equipos.
- [E.24] Caída del sistema por agotamiento de recursos.
- [E.25] Pérdida de equipos.
- [E.28] Indisponibilidad del personal.

- Ataques intencionados.- [A] Amenazas con tintes intencionados, provocados por humanos.
    - [A.3]Manipulación de los registros de actividad (log)
    - [A.4]Manipulación de la configuración
    - [A.5]Suplantación de la identidad del usuario
    - [A.6]Abuso de privilegios de acceso
    - [A.7]Uso no previsto
    - [A.8]Difusión de software dañino
    - [A.9] [Re-]encaminamiento de mensajes
    - [A.10]Alteración de secuencia
    - [A.11]Acceso no autorizado
    - [A.12]Análisis de tráfico
    - [A.13]Repudio
    - [A.14]Interceptación de información (escucha)
    - [A.15]Modificación deliberada de la información
    - [A.18]Destrucción de información
    - [A.19]Divulgación de información
    - [A.22]Manipulación de programas
    - [A.23]Manipulación de los equipos
    - [A.24]Denegación de servicio
    - [A.25]Robo
    - [A.26]Ataque destructivo
    - [A.27]Ocupación enemiga
    - [A.28]Indisponibilidad del personal
    - [A.29]Extorsión
    - [A.30]Ingeniería social (picaresca)

| HARDWARE | | | | |
|---|---|---|---|---|
| **[HW] - ACC DE PRECISIÓN.** | **FA** | **35%** | **50%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FMB | | | 100% |
| [I.5] Avería de origen físico o lógico | FB | | | 100% |
| [I.6] Corte del suministro eléctrico | FM | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FB | | | 100% |
| [E.2] Errores del administrador | FMB | 10% | 50% | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FB | | | 100% |
| [E.25] Pérdida de equipos | FMB | | | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 25% | 50% | 100% |
| [A.7] Uso no previsto | FMB | 25% | 50% | 100% |
| [A.11] Acceso no autorizado | FMB | 25% | 50% | |
| [A.23] Manipulación de los equipos | FMB | 25% | | 100% |
| [A.24] Denegación de servicio | FMB | | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] - CABLEADO ESTRUCTURADO.** | **FMB** | **55%** | **50%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FMB | | | 100% |
| [I.5] Avería de origen físico o lógico | FB | | | 100% |
| [I.6] Corte del suministro eléctrico | FM | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FB | | | 100% |
| [E.2] Errores del administrador | FMB | 100% | 100% | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |

| | | | | |
|---|---|---|---|---|
| [E.24] Caída del sistema por agotamiento de recursos | FB | | | 100% |
| [E.25] Pérdida de equipos | FMB | | | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | | | |
| [A.7] Uso no previsto | FMB | 25% | 25% | 100% |
| [A.11] Acceso no autorizado | FMB | 25% | 25% | |
| [A.23] Manipulación de los equipos | FMB | 25% | | 100% |
| [A.24] Denegación de servicio | FMB | | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] - CCTV** | **FMB** | **35%** | **30%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FMB | | | 100% |
| [I.5] Avería de origen físico o lógico | FB | | | 100% |
| [I.6] Corte del suministro eléctrico | FM | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FB | | | 100% |
| [E.2] Errores del administrador | FMB | 10% | 50% | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FB | | | 100% |
| [E.25] Pérdida de equipos | FMB | | | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 25% | 25% | 100% |
| [A.7] Uso no previsto | FMB | 25% | 20% | 100% |
| [A.11] Acceso no autorizado | FMB | 25% | 25% | |
| [A.23] Manipulación de los equipos | FMB | 25% | | 100% |
| [A.24] Denegación de servicio | FMB | | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] - BIOMÉTRICOS (ACCESO Y ASISTENCIA)** | **FM** | **45%** | **35%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FB | | | 100% |

| | | | | |
|---|---|---|---|---|
| [I.5] Avería de origen físico o lógico | FM | | | 100% |
| [I.6] Corte del suministro eléctrico | FB | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FMB | 15% | 50% | 100% |
| [E.2] Errores del administrador | FB | | | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FMB | | | 100% |
| [E.25] Pérdida de equipos | FMB | 25% | 25% | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 25% | 40% | 100% |
| [A.7] Uso no previsto | FMB | 25% | 25% | |
| [A.11] Acceso no autorizado | FMB | 25% | | 100% |
| [A.23] Manipulación de los equipos | FMB | | | 100% |
| [A.24] Denegación de servicio | FMB | 100% | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] - DISPOSITIVOS TELEFÓNICOS.** | **FMB** | **50%** | **40%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FB | | | 100% |
| [I.5] Avería de origen físico o lógico | FM | | | 100% |
| [I.6] Corte del suministro eléctrico | FB | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FMB | 10% | 60% | 100% |
| [E.2] Errores del administrador | FB | | | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FMB | | | 100% |
| [E.25] Pérdida de equipos | FMB | 35% | 50% | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 35% | 25% | 100% |
| [A.7] Uso no previsto | FMB | 25% | 25% | |
| [A.11] Acceso no autorizado | FMB | 45% | | 100% |
| [A.23] Manipulación de los equipos | FMB | | | 100% |
| [A.24] Denegación de servicio | FMB | 100% | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] - EQUIPOS DE RED . (ACCESS POINT, SWITCH )** | **FB** | **50%** | **35%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| [N.1] Fuego | FMB | | | 100% |

| | | | | |
|---|---|---|---|---|
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FB | | | 100% |
| [I.5] Avería de origen físico o lógico | FM | | | 100% |
| [I.6] Corte del suministro eléctrico | FB | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FMB | 50% | 50% | 100% |
| [E.2] Errores del administrador | FB | | | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FMB | | | 100% |
| [E.25] Pérdida de equipos | FMB | 25% | 20% | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 25% | 20% | 100% |
| [A.7] Uso no previsto | FMB | 25% | 50% | |
| [A.11] Acceso no autorizado | FMB | 25% | | 100% |
| [A.23] Manipulación de los equipos | FMB | | | 100% |
| [A.24] Denegación de servicio | FMB | 100% | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] -ESTACIONES DE TRABAJO** | **FM** | **50%** | **50%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FB | | | 100% |
| [I.5] Avería de origen físico o lógico | FM | | | 100% |
| [I.6] Corte del suministro eléctrico | FB | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FMB | 50% | 50% | 100% |
| [E.2] Errores del administrador | FB | | | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FMB | | | 100% |
| [E.25] Pérdida de equipos | FMB | 25% | 50% | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 25% | 50% | 100% |
| [A.7] Uso no previsto | FMB | 25% | 50% | |
| [A.11] Acceso no autorizado | FMB | 25% | | 100% |

| | | | | |
|---|---|---|---|---|
| [A.23] Manipulación de los equipos | FMB | | | 100% |
| [A.24] Denegación de servicio | FMB | 100% | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] - FIREWALLS** | **FM** | **50%** | **25%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FB | | | 100% |
| [I.5] Avería de origen físico o lógico | FM | | | 100% |
| [I.6] Corte del suministro eléctrico | FB | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FMB | 50% | 25% | 100% |
| [E.2] Errores del administrador | FB | | | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FMB | | | 100% |
| [E.25] Pérdida de equipos | FMB | 25% | 25% | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 25% | 25% | 100% |
| [A.7] Uso no previsto | FMB | 25% | 25% | |
| [A.11] Acceso no autorizado | FMB | 25% | | 100% |
| [A.23] Manipulación de los equipos | FMB | | | 100% |
| [A.24] Denegación de servicio | FMB | 100% | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] - IMPRESORAS** | **FMB** | **50%** | **50%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FB | | | 100% |
| [I.5] Avería de origen físico o lógico | FM | | | 100% |
| [I.6] Corte del suministro eléctrico | FB | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FMB | 50% | 50% | 100% |
| [E.2] Errores del administrador | FB | | | 100% |

| | | | | |
|---|---|---|---|---|
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FMB | | | 100% |
| [E.25] Pérdida de equipos | FMB | 25% | 50% | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 25% | 50% | 100% |
| [A.7] Uso no previsto | FMB | 25% | 50% | |
| [A.11] Acceso no autorizado | FMB | 25% | | 100% |
| [A.23] Manipulación de los equipos | FMB | | | 100% |
| [A.24] Denegación de servicio | FMB | 100% | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] - ROUTERS** | **FB** | **55%** | **25%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FB | | | 100% |
| [I.5] Avería de origen físico o lógico | FM | | | 100% |
| [I.6] Corte del suministro eléctrico | FB | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FMB | 30% | 25% | 100% |
| [E.2] Errores del administrador | FB | | | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FMB | | | 100% |
| [E.25] Pérdida de equipos | FMB | 30% | 25% | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 25% | 25% | 100% |
| [A.7] Uso no previsto | FMB | 50% | 25% | |
| [A.11] Acceso no autorizado | FMB | 50% | | 100% |
| [A.23] Manipulación de los equipos | FMB | | | 100% |
| [A.24] Denegación de servicio | FMB | 100% | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] - SERVIDOR DE ARCHIVOS. (NAS)** | **FA** | **100%** | **80%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |

| | | | | |
|---|---|---|---|---|
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FB | | | 100% |
| [I.5] Avería de origen físico o lógico | FM | | | 100% |
| [I.6] Corte del suministro eléctrico | FB | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FMB | 100% | 100% | 100% |
| [E.2] Errores del administrador | FB | 100% | 100% | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FMB | | | 100% |
| [E.25] Pérdida de equipos | FMB | 100% | | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 100% | 50% | 100% |
| [A.7] Uso no previsto | FMB | 100% | 50% | 100% |
| [A.11] Acceso no autorizado | FMB | 100% | 100% | |
| [A.23] Manipulación de los equipos | FMB | 100% | | 100% |
| [A.24] Denegación de servicio | FMB | 100% | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] - SERVIDOR DE CORREO ELECTRÓNICO.** | **FA** | **95%** | **80%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FB | | | 100% |
| [I.5] Avería de origen físico o lógico | FM | | | 100% |
| [I.6] Corte del suministro eléctrico | FB | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FMB | 55% | 100% | 100% |
| [E.2] Errores del administrador | FB | 100% | 100% | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FMB | | | 100% |
| [E.25] Pérdida de equipos | FMB | 100% | | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 100% | 50% | 100% |
| [A.7] Uso no previsto | FMB | 100% | 50% | 100% |
| [A.11] Acceso no autorizado | FMB | 100% | 100% | |
| [A.23] Manipulación de los equipos | FMB | 100% | | 100% |
| [A.24] Denegación de servicio | FMB | 100% | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] - SERVIDOR DE TELEFONÍA IP.** | **FMB** | **90%** | **80%** | **100%** |

| LISTA DE AMENAZAS | FREC | C | I | D |
|---|---|---|---|---|
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FB | | | 100% |
| [I.5] Avería de origen físico o lógico | FM | | | 100% |
| [I.6] Corte del suministro eléctrico | FB | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FMB | 10% | 100% | 100% |
| [E.2] Errores del administrador | FB | 100% | 100% | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FMB | | | 100% |
| [E.25] Pérdida de equipos | FMB | 100% | | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 100% | 50% | 100% |
| [A.7] Uso no previsto | FMB | 100% | 50% | 100% |
| [A.11] Acceso no autorizado | FMB | 100% | 100% | |
| [A.23] Manipulación de los equipos | FMB | 100% | | 100% |
| [A.24] Denegación de servicio | FMB | 100% | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] - SERVIDOR GEORREFERENCIACIÓN. (GIS)** | **FB** | **90%** | **80%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FB | | | 100% |
| [I.5] Avería de origen físico o lógico | FM | | | 100% |
| [I.6] Corte del suministro eléctrico | FB | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FMB | 10% | 100% | 100% |
| [E.2] Errores del administrador | FB | 100% | 100% | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FMB | | | 100% |
| [E.25] Pérdida de equipos | FMB | 100% | | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 100% | 50% | 100% |

| | | | | |
|---|---|---|---|---|
| [A.7] Uso no previsto | FMB | 100% | 50% | 100% |
| [A.11] Acceso no autorizado | FMB | 100% | 100% | |
| [A.23] Manipulación de los equipos | FMB | 100% | | 100% |
| [A.24] Denegación de servicio | FMB | 100% | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] - SERVIDORES DE AUTÓMATAS (SCADA).** | **FB** | **90%** | **80%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FB | | | 100% |
| [I.5] Avería de origen físico o lógico | FM | | | 100% |
| [I.6] Corte del suministro eléctrico | FB | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FMB | 10% | 100% | 100% |
| [E.2] Errores del administrador | FB | 100% | 100% | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FMB | | | 100% |
| [E.25] Pérdida de equipos | FMB | 100% | | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 100% | 50% | 100% |
| [A.7] Uso no previsto | FMB | 100% | 50% | 100% |
| [A.11] Acceso no autorizado | FMB | 100% | 100% | |
| [A.23] Manipulación de los equipos | FMB | 100% | | 100% |
| [A.24] Denegación de servicio | FMB | 100% | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] - SERVIDOR VIRTUALIZACIÓN.** | **FB** | **90%** | **80%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FB | | | 100% |
| [I.5] Avería de origen físico o lógico | FM | | | 100% |
| [I.6] Corte del suministro eléctrico | FB | | | 100% |

| | | | | |
|---|---|---|---|---|
| [I.7] Condiciones inadecuadas de temperatura o humedad | FMB | 10% | 100% | 100% |
| [E.2] Errores del administrador | FB | 100% | 100% | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FMB | | | 100% |
| [E.25] Pérdida de equipos | FMB | 100% | | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 100% | 50% | 100% |
| [A.7] Uso no previsto | FMB | 100% | 50% | 100% |
| [A.11] Acceso no autorizado | FMB | 100% | 100% | |
| [A.23] Manipulación de los equipos | FMB | 100% | | 100% |
| [A.24] Denegación de servicio | FMB | 100% | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **[HW] - UPS** | **FA** | **90%** | **80%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | D |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.3] Contaminación mecánica | FMB | | | 100% |
| [I.4] Contaminación electromagnética | FMB | | | 100% |
| [I.5] Avería de origen físico o lógico | FB | | | 100% |
| [I.6] Corte del suministro eléctrico | FM | | | 100% |
| [I.7] Condiciones inadecuadas de temperatura o humedad | FB | | | 100% |
| [E.2] Errores del administrador | FMB | 80% | 80% | 100% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardware) | FB | | | 100% |
| [E.24] Caída del sistema por agotamiento de recurso | FB | | | 100% |
| [E.25] Pérdida de equipos | FMB | | | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 80% | 80% | 100% |
| [A.7] Uso no previsto | FMB | 100% | 80% | 100% |
| [A.11] Acceso no autorizado | FMB | 80% | 80% | |
| [A.23] Manipulación de los equipos | FMB | 100% | | 100% |
| [A.24] Denegación de servicio | FMB | | | 100% |
| [A.25] Robo | FMB | 100% | | 100% |
| [A.26] Ataque destructivo | FMB | | | 100% |
| **SOFTWARE** | | | | |
| **[SW] - ANTIVIRUS** | **FA** | **85%** | **100%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [i.5] Avería de origen físico o lógico | FM | | | 100% |

| | | | | |
|---|---|---|---|---|
| [E.1] Errores de los usuarios | FA | 25% | 100% | 100% |
| [E.2] Errores del administrador | FM | 25% | 100% | 100% |
| [E.8] Difusión de SW dañino | FMA | 100% | 100% | 100% |
| [E.9] Errores de [re]-encaminamiento | FB | 50% | | |
| [E.10] Errores de secuencia | FMB | | 100% | |
| [E.15] Alteración accidental de la información | FB | | 100% | |
| [E.18] Destrucción de la información | FB | | | 100% |
| [E.19] Fugas de información | FA | 100% | | |
| [E.20] Vulnerabilidades de los programas (SW) | FB | 100% | 100% | 100% |
| [E.21] Errores de mantenimiento / actualización de programas (SW) | FB | | 100% | 100% |
| [A.5]Suplantación de la identidad del usuario | FB | 100% | 100% | |
| [A.6]Abuso de privilegios de acceso | FA | 100% | 100% | 100% |
| [A.7]Uso no previsto | FA | 100% | 100% | 100% |
| [A.8]Difusión de software dañino | FMB | 100% | 100% | 100% |
| [A.9] [Re-]encaminamiento de mensajes | FMB | | | 100% |
| [A.10]Alteración de secuencia | FMB | | 100% | |
| [A.11]Acceso no autorizado | FB | 100% | 100% | |
| [A.15]Modificación deliberada de la información | FM | | 100% | |
| [A.18]Destrucción de información | FMB | | | 100% |
| [A.19]Divulgación de información | FB | 100% | | |
| [A.22]Manipulación de programas | FB | 100% | 100% | 100% |
| **[SW] - APLICACIONES INTERNAS.** | **FA** | **90%** | **100%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [i.5] Avería de origen físico o lógico | FM | | | 100% |
| [E.1] Errores de los usuarios | FA | 100% | 100% | 100% |
| [E.2] Errores del administrador | FM | 100% | 100% | 100% |
| [E.8] Difusión de SW dañino | FMB | 100% | 100% | 100% |
| [E.9] Errores de [re]-encaminamiento | FMB | 50% | | |
| [E.10] Errores de secuencia | FMB | | 100% | |
| [E.15] Alteración accidental de la información | FB | | 100% | |
| [E.18] Destrucción de la información | FB | | | 100% |
| [E.19] Fugas de información | FA | 100% | | |
| [E.20] Vulnerabilidades de los programas (SW) | FB | 100% | 100% | 100% |
| [E.21] Errores de mantenimiento / actualización de programas (SW) | FB | | 100% | 100% |
| [A.5]Suplantación de la identidad del usuario | FB | 100% | 100% | |
| [A.6]Abuso de privilegios de acceso | FA | 100% | 100% | 100% |
| [A.7]Uso no previsto | FA | 100% | 100% | 100% |
| [A.8]Difusión de software dañino | FMB | 100% | 100% | 100% |
| [A.9] [Re-]encaminamiento de mensajes | FMB | | | 100% |
| [A.10]Alteración de secuencia | FMB | | 100% | |
| [A.11]Acceso no autorizado | FB | 100% | 100% | |
| [A.15]Modificación deliberada de la información | FM | | 100% | |
| [A.18]Destrucción de información | FMB | | | 100% |

| | | | | |
|---|---|---|---|---|
| [A.19]Divulgación de información | FB | 25% | | |
| [A.22]Manipulación de programas | FB | 100% | 100% | 100% |
| **[SW] - HERRAMIENTAS DE DESARROLLO** | **FA** | **90%** | **100%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [i.5] Avería de origen físico o lógico | FM | | | 100% |
| [E.1] Errores de los usuarios | FA | 100% | 100% | 100% |
| [E.2] Errores del administrador | FM | 100% | 100% | 100% |
| [E.8] Difusión de SW dañino | FMB | 100% | 100% | 100% |
| [E.9] Errores de [re]-encaminamiento | FMB | 50% | | |
| [E.10] Errores de secuencia | FMB | | 100% | |
| [E.15] Alteración accidental de la información | FB | | 100% | |
| [E.18] Destrucción de la información | FB | | | 100% |
| [E.19] Fugas de información | FA | 100% | | |
| [E.20] Vulnerabilidades de los programas (SW) | FB | 100% | 100% | 100% |
| [E.21] Errores de mantenimiento / actualización de programas (SW) | FB | | 100% | 100% |
| [A.5]Suplantación de la identidad del usuario | FB | 100% | 100% | |
| [A.6]Abuso de privilegios de acceso | FA | 100% | 100% | 100% |
| [A.7]Uso no previsto | FA | 100% | 100% | 100% |
| [A.8]Difusión de software dañino | FMB | 100% | 100% | 100% |
| [A.9] [Re-]encaminamiento de mensajes | FMB | | | 100% |
| [A.10]Alteración de secuencia | FMB | | 100% | |
| [A.11]Acceso no autorizado | FB | 100% | 100% | |
| [A.15]Modificación deliberada de la información | FM | | 100% | |
| [A.18]Destrucción de información | FMB | | | 100% |
| [A.19]Divulgación de información | FB | 25% | | |
| [A.22]Manipulación de programas | FB | 100% | 100% | 100% |
| **[SW] - PROGRAMAS UTILITARIOS** | **FM** | **90%** | **90%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [i.5] Avería de origen físico o lógico | FM | | | 100% |
| [E.1] Errores de los usuarios | FA | 100% | 100% | 100% |
| [E.2] Errores del administrador | FM | 100% | 100% | 100% |
| [E.8] Difusión de SW dañino | FMB | 100% | 100% | 100% |
| [E.9] Errores de [re]-encaminamiento | FMB | 50% | | |
| [E.10] Errores de secuencia | FMB | | 30% | |
| [E.15] Alteración accidental de la información | FB | | 100% | |
| [E.18] Destrucción de la información | FB | | | 100% |
| [E.19] Fugas de información | FA | 100% | | |
| [E.20] Vulnerabilidades de los programas (SW) | FB | 100% | 100% | 100% |
| [E.21] Errores de mantenimiento / actualización de programas (SW) | FB | | 100% | 100% |
| [A.5]Suplantación de la identidad del usuario | FB | 100% | 25% | |
| [A.6]Abuso de privilegios de acceso | FA | 100% | 100% | 100% |
| [A.7]Uso no previsto | FA | 100% | 100% | 100% |
| [A.8]Difusión de software dañino | FMB | 100% | 100% | 100% |

| | | | | |
|---|---|---|---|---|
| [A.9] [Re-]encaminamiento de mensajes | FMB | | | 100% |
| [A.10]Alteración de secuencia | FMB | | 100% | |
| [A.11]Acceso no autorizado | FB | 100% | 100% | |
| [A.15]Modificación deliberada de la información | FM | | 100% | |
| [A.18]Destrucción de información | FMB | | | 100% |
| [A.19]Divulgación de información | FB | 25% | | |
| [A.22]Manipulación de programas | FB | 100% | 100% | 100% |
| **[SW] - SISTEMAS OPERATIVOS** | **FM** | **90%** | **90%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [i.5] Avería de origen físico o lógico | FM | | | 100% |
| [E.1] Errores de los usuarios | FA | 100% | 100% | 100% |
| [E.2] Errores del administrador | FM | 100% | 100% | 100% |
| [E.8] Difusión de SW dañino | FMB | 100% | 100% | 100% |
| [E.9] Errores de [re]-encaminamiento | FMB | 50% | | |
| [E.10] Errores de secuencia | FMB | | 30% | |
| [E.15] Alteración accidental de la información | FB | | 100% | |
| [E.18] Destrucción de la información | FB | | | 100% |
| [E.19] Fugas de información | FA | 100% | | |
| [E.20] Vulnerabilidades de los programas (SW) | FB | 100% | 100% | 100% |
| [E.21] Errores de mantenimiento / actualización de programas (SW) | FB | | 100% | 100% |
| [A.5]Suplantación de la identidad del usuario | FB | 100% | 25% | |
| [A.6]Abuso de privilegios de acceso | FA | 100% | 100% | 100% |
| [A.7]Uso no previsto | FA | 100% | 100% | 100% |
| [A.8]Difusión de software dañino | FMB | 100% | 100% | 100% |
| [A.9] [Re-]encaminamiento de mensajes | FMB | | | 100% |
| [A.10]Alteración de secuencia | FMB | | 100% | |
| [A.11]Acceso no autorizado | FB | 100% | 100% | |
| [A.15]Modificación deliberada de la información | FM | | 100% | |
| [A.18]Destrucción de información | FMB | | | 100% |
| [A.19]Divulgación de información | FB | 25% | | |
| [A.22]Manipulación de programas | FB | 100% | 100% | 100% |
| **[SW] - SW CORREO ELECTRÓNICO** | **FM** | **85%** | **100%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [i.5] Avería de origen físico o lógico | FM | | | 100% |
| [E.1] Errores de los usuarios | FA | 25% | 100% | 100% |
| [E.2] Errores del administrador | FM | 25% | 100% | 100% |
| [E.8] Difusión de SW dañino | FMA | 100% | 100% | 100% |
| [E.9] Errores de [re]-encaminamiento | FB | 50% | | |
| [E.10] Errores de secuencia | FMB | | 100% | |
| [E.15] Alteración accidental de la información | FB | | 100% | |
| [E.18] Destrucción de la información | FB | | | 100% |
| [E.19] Fugas de información | FA | 100% | | |
| [E.20] Vulnerabilidades de los programas (SW) | FB | 100% | 100% | 100% |

| | | | | |
|---|---|---|---|---|
| [E.21] Errores de mantenimiento / actualización de programas (SW) | FB | | 100% | 100% |
| [A.5]Suplantación de la identidad del usuario | FB | 100% | 100% | |
| [A.6]Abuso de privilegios de acceso | FA | 100% | 100% | 100% |
| [A.7]Uso no previsto | FA | 100% | 100% | 100% |
| [A.8]Difusión de software dañino | FMB | 100% | 100% | 100% |
| [A.9] [Re-]encaminamiento de mensajes | FMB | | | 100% |
| [A.10]Alteración de secuencia | FMB | | 100% | |
| [A.11]Acceso no autorizado | FB | 100% | 100% | |
| [A.15]Modificación deliberada de la información | FM | | 100% | |
| [A.18]Destrucción de información | FMB | | | 100% |
| [A.19]Divulgación de información | FB | 100% | | |
| [A.22]Manipulación de programas | FB | 100% | 100% | 100% |
| **[SW] - SW VIRTUALIZACIÓN** | **FM** | **85%** | **100%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [i.5] Avería de origen físico o lógico | FM | | | 100% |
| [E.1] Errores de los usuarios | FA | 25% | 100% | 100% |
| [E.2] Errores del administrador | FM | 25% | 100% | 100% |
| [E.8] Difusión de SW dañino | FMA | 100% | 100% | 100% |
| [E.9] Errores de [re]-encaminamiento | FB | 50% | | |
| [E.10] Errores de secuencia | FMB | | 100% | |
| [E.15] Alteración accidental de la información | FB | | 100% | |
| [E.18] Destrucción de la información | FB | | | 100% |
| [E.19] Fugas de información | FA | 100% | | |
| [E.20] Vulnerabilidades de los programas (SW) | FB | 100% | 100% | 100% |
| [E.21] Errores de mantenimiento / actualización de programas (SW) | FB | | 100% | 100% |
| [A.5]Suplantación de la identidad del usuario | FB | 100% | 100% | |
| [A.6]Abuso de privilegios de acceso | FA | 100% | 100% | 100% |
| [A.7]Uso no previsto | FA | 100% | 100% | 100% |
| [A.8]Difusión de software dañino | FMB | 100% | 100% | 100% |
| [A.9] [Re-]encaminamiento de mensajes | FMB | | | 100% |
| [A.10]Alteración de secuencia | FMB | | 100% | |
| [A.11]Acceso no autorizado | FB | 100% | 100% | |
| [A.15]Modificación deliberada de la información | FM | | 100% | |
| [A.18]Destrucción de información | FMB | | | 100% |
| [A.19]Divulgación de información | FB | 100% | | |
| [A.22]Manipulación de programas | FB | 100% | 100% | 100% |
| **[SW] - SW SCADA** | **FB** | **85%** | **100%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [i.5] Avería de origen físico o lógico | FM | | | 100% |
| [E.1] Errores de los usuarios | FA | 25% | 100% | 100% |
| [E.2] Errores del administrador | FM | 25% | 100% | 100% |
| [E.8] Difusión de SW dañino | FMA | 100% | 100% | 100% |
| [E.9] Errores de [re]-encaminamiento | FB | 50% | | |

| | | | | |
|---|---|---|---|---|
| [E.10] Errores de secuencia | FMB | | 100% | |
| [E.15] Alteración accidental de la información | FB | | 100% | |
| [E.18] Destrucción de la información | FB | | | 100% |
| [E.19] Fugas de información | FA | 100% | | |
| [E.20] Vulnerabilidades de los programas (SW) | FB | 100% | 100% | 100% |
| [E.21] Errores de mantenimiento / actualización de programas (SW) | FB | | 100% | 100% |
| [A.5]Suplantación de la identidad del usuario | FB | 100% | 100% | |
| [A.6]Abuso de privilegios de acceso | FA | 100% | 100% | 100% |
| [A.7]Uso no previsto | FA | 100% | 100% | 100% |
| [A.8]Difusión de software dañino | FMB | 100% | 100% | 100% |
| [A.9] [Re-]encaminamiento de mensajes | FMB | | | 100% |
| [A.10]Alteración de secuencia | FMB | | 100% | |
| [A.11]Acceso no autorizado | FB | 100% | 100% | |
| [A.15]Modificación deliberada de la información | FM | | 100% | |
| [A.18]Destrucción de información | FMB | | | 100% |
| [A.19]Divulgación de información | FB | 100% | | |
| [A.22]Manipulación de programas | FB | 100% | 100% | 100% |
| **PERSONAL.** | | | | |
| **[P] - ALTA GERENCIA** | **FM** | **60%** | **50%** | **55%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.19] Fugas de información | FA | 80% | | |
| [E.28] Indisponibilidad del personal | FA | | | 50% |
| [A.28] Indisponibilidad del personal | FM | | | 50% |
| [A.29] Extorsión | FM | 50% | 50% | 50% |
| [A.30] Ingeniería social(picaresca) | FM | 50% | 50% | 70% |
| **[P] - CONTROL DE ACCESOS (GUARDIANÍA)** | **FM** | **50%** | **30%** | **30%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.19] Fugas de información | FB | 50% | | |
| [E.28] Indisponibilidad del personal | FMB | | | 20% |
| [A.28] Indisponibilidad del personal | FB | | | 20% |
| [A.29] Extorsión | FM | 50% | 10% | 30% |
| [A.30] Ingeniería social(picaresca) | FM | 50% | 50% | 50% |
| **[P] - DESARROLLADORES DE SOFTWARE.** | **FA** | **100%** | **80%** | **80%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.19] Fugas de información | FM | 100% | | |
| [E.28] Indisponibilidad del personal | FM | | | 60% |
| [A.28] Indisponibilidad del personal | FMB | | | 60% |
| [A.29] Extorsión | FM | 100% | 80% | 100% |
| [A.30] Ingeniería social(picaresca) | FMB | 100% | 80% | 100% |
| **[P] - PERSONAL EXTERNO.** | **FM** | **50%** | **30%** | **30%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.19] Fugas de información | FB | 50% | | |
| [E.28] Indisponibilidad del personal | FMB | | | 20% |
| [A.28] Indisponibilidad del personal | FMB | | | 20% |

| | | | | |
|---|---|---|---|---|
| [A.29] Extorsión | FB | 50% | 10% | 30% |
| [A.30] Ingeniería social(picaresca) | FM | 50% | 50% | 50% |
| **[P] - PERSONAL OPERATIVO.** | **FM** | **50%** | **30%** | **30%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.19] Fugas de información | FB | 50% | | |
| [E.28] Indisponibilidad del personal | FMB | | | 20% |
| [A.28] Indisponibilidad del personal | FB | | | 20% |
| [A.29] Extorsión | FM | 50% | 10% | 30% |
| [A.30] Ingeniería social(picaresca) | FM | 50% | 50% | 50% |
| **[P] - PERSONAL TECNOLÓGICO (INFRAESTRUCTURA-SOPORTE)** | **FA** | **100%** | **80%** | **80%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.19] Fugas de información | FM | 100% | | |
| [E.28] Indisponibilidad del personal | FM | | | 60% |
| [A.28] Indisponibilidad del personal | FMB | | | 60% |
| [A.29] Extorsión | FM | 100% | 80% | 100% |
| [A.30] Ingeniería social(picaresca) | FMB | 100% | 80% | 100% |
| **[P] - USUARIOS FINALES.** | **FA** | **100%** | **80%** | **80%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.19] Fugas de información | FM | 100% | | |
| [E.28] Indisponibilidad del personal | FM | | | 60% |
| [A.28] Indisponibilidad del personal | FMB | | | 60% |
| [A.29] Extorsión | FM | 100% | 80% | 100% |
| [A.30] Ingeniería social(picaresca) | FMB | 100% | 80% | 100% |
| **INFRAESTRUCTURA** | | | | |
| **[L] - CENTRO DE DATOS** | **FM** | **60%** | **55%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.11] Emanaciones electromagnéticas. | FMB | 80% | | |
| [E.15] Alteración accidental de la información | FB | | 100% | |
| [E.18] Destrucción de información | FMB | | | 100% |
| [E.19] Fugas de información | FB | 80% | | |
| [A.7] Uso no previsto | FB | 50% | 50% | 100% |
| [A.11] Acceso no autorizado | FMB | 50% | 20% | |
| [A.15] Modificación deliberada de la información | FMB | | 50% | |
| [A.18] Destrucción de información | FMB | | | 100% |
| [A.19] Divulgación de información. | FMB | 50% | | |
| [A.26] Ataque destructivo | FMB | | | 100% |
| [A.27] Ocupación enemiga | FMB | 50% | | 100% |
| **[L] - CENTRO DE MONITOREO (CONTROL SCADA).** | **FM** | **60%** | **55%** | **100%** |

| LISTA DE AMENAZAS | FREC | C | I | D |
|---|---|---|---|---|
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.11] Emanaciones electromagnéticas. | FMB | 80% | | |
| [E.15] Alteración accidental de la información | FB | | 100% | |
| [E.18] Destrucción de información | FMB | | | 100% |
| [E.19] Fugas de información | FB | 80% | | |
| [A.7] Uso no previsto | FB | 50% | 50% | 100% |
| [A.11] Acceso no autorizado | FMB | 50% | 20% | |
| [A.15] Modificación deliberada de la información | FMB | | 50% | |
| [A.18] Destrucción de información | FMB | | | 100% |
| [A.19] Divulgación de información. | FMB | 50% | | |
| [A.26] Ataque destructivo | FMB | | | 100% |
| [A.27] Ocupación enemiga | FMB | 50% | | 100% |
| **[L] - INSTALACIONES ESTRUCTURALES. (EDIFICIO, SEDES)** | **FB** | **60%** | **55%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.11] Emanaciones electromagnéticas. | FMB | 80% | | |
| [E.15] Alteración accidental de la información | FB | | 100% | |
| [E.18] Destrucción de información | FMB | | | 100% |
| [E.19] Fugas de información | FB | 80% | | |
| [A.7] Uso no previsto | FB | 50% | 50% | 100% |
| [A.11] Acceso no autorizado | FMB | 50% | 20% | |
| [A.15] Modificación deliberada de la información | FMB | | 50% | |
| [A.18] Destrucción de información | FMB | | | 100% |
| [A.19] Divulgación de información. | FMB | 50% | | |
| [A.26] Ataque destructivo | FMB | | | 100% |
| [A.27] Ocupación enemiga | FMB | 50% | | 100% |
| **[L] - LABORATORIOS DE AGUA POTABLE.** | **FB** | **60%** | **55%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |

| | | | | |
|---|---|---|---|---|
| [I.11] Emanaciones electromagnéticas. | FMB | 80% | | |
| [E.15] Alteración accidental de la información | FB | | 100% | |
| [E.18] Destrucción de información | FMB | | | 100% |
| [E.19] Fugas de información | FB | 80% | | |
| [A.7] Uso no previsto | FB | 50% | 50% | 100% |
| [A.11] Acceso no autorizado | FMB | 50% | 20% | |
| [A.15] Modificación deliberada de la información | FMB | | 50% | |
| [A.18] Destrucción de información | FMB | | | 100% |
| [A.19] Divulgación de información. | FMB | 50% | | |
| [A.26] Ataque destructivo | FMB | | | 100% |
| [A.27] Ocupación enemiga | FMB | 50% | | 100% |
| **[L] - PLANTAS DE BOMBEO Y TRATAMIENTO.** | **FB** | **60%** | **55%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [N.1] Fuego | FMB | | | 100% |
| [N.2] Daños por agua | FMB | | | 100% |
| [N.*] Desastres naturales | FMB | | | 100% |
| [I.1] Fuego | FMB | | | 100% |
| [I.2] Daños por agua | FMB | | | 100% |
| [I.*] Desastres industriales | FMB | | | 100% |
| [I.11] Emanaciones electromagnéticas. | FMB | 80% | | |
| [E.15] Alteración accidental de la información | FB | | 100% | |
| [E.18] Destrucción de información | FMB | | | 100% |
| [E.19] Fugas de información | FB | 80% | | |
| [A.7] Uso no previsto | FB | 50% | 50% | 100% |
| [A.11] Acceso no autorizado | FMB | 50% | 20% | |
| [A.15] Modificación deliberada de la información | FMB | | 50% | |
| [A.18] Destrucción de información | FMB | | | 100% |
| [A.19] Divulgación de información. | FMB | 50% | | |
| [A.26] Ataque destructivo | FMB | | | 100% |
| [A.27] Ocupación enemiga | FMB | 50% | | 100% |
| **SERVICIOS** | | | | |
| **[S] - CORREO ELECTRÓNICO.** | **FA** | **70%** | **70%** | **90%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.1] Errores de los usuarios | FMA | 100% | 100% | 100% |
| [E.2] Errores del administrador | FB | 100% | 100% | 100% |
| [E.9] Errores de [re]-encaminamiento | FB | 50% | | |
| [E.10] Errores de secuencia | FMB | | 50% | |
| [E.15] Alteración accidental de la información | FB | | 50% | |
| [E.18] Destrucción de la información | FB | | | 100% |
| [E.19] Fugas de información | FB | | | 50% |
| [E.24] Caída del sistema por agotamiento de recursos | FB | | | 100% |
| [A.5] Suplantación de la identidad del usuario | FA | 100% | 100% | 100% |
| [A.6] Abuso de privilegios de acceso | FMB | 100% | 60% | 100% |
| [A.7] Uso no previsto | FB | 50% | 60% | 50% |
| [A.9] [Re-]encaminamiento de mensajes | FMB | 50% | | |

| | | | | |
|---|---|---|---|---|
| [A.10] Alteración de secuencia | FMB | | 50% | |
| [A.11] Acceso no autorizado | FM | 30% | 50% | |
| [A.13] Repudio | FB | | 100% | |
| [A.15] Modificación deliberada de la información | FB | | 50% | |
| [A.18] Destrucción de información | FB | | | 100% |
| [A.19] Divulgación de información | FB | 50% | | |
| [A.24] Denegación de servicio | FMB | | | 100% |
| **[S] - INFRAESTRUCTURA CLOUD** | **FA** | **40%** | **45%** | **45%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.1] Errores de los usuarios | FB | 30% | 50% | 20% |
| [E.2] Errores del administrador | FB | 30% | 50% | 20% |
| [E.9] Errores de [re]-encaminamiento | FMB | 50% | | |
| [E.10] Errores de secuencia | FMB | | 50% | |
| [E.15] Alteración accidental de la información | FB | | 50% | |
| [E.18] Destrucción de la información | FMB | | | 20% |
| [E.19] Fugas de información | FB | | | 50% |
| [E.24] Caída del sistema por agotamiento de recursos | FM | | | 100% |
| [A.5] Suplantación de la identidad del usuario | FMB | 30% | 20% | 20% |
| [A.6] Abuso de privilegios de acceso | FMB | 30% | 20% | 20% |
| [A.7] Uso no previsto | FB | 30% | 50% | 50% |
| [A.9] [Re-]encaminamiento de mensajes | FMB | 50% | | |
| [A.10] Alteración de secuencia | FMB | | 50% | |
| [A.11] Acceso no autorizado | FMB | 60% | 50% | |
| [A.13] Repudio | FMB | | 50% | |
| [A.15] Modificación deliberada de la información | FMB | | 50% | |
| [A.18] Destrucción de información | FMB | | | 50% |
| [A.19] Divulgación de información | FMB | 50% | | |
| [A.24] Denegación de servicio | FB | | | 100% |
| **[S] - PORTALES TECNOLÓGICOS PUBLICADOS** | **FA** | **40%** | **45%** | **45%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.1] Errores de los usuarios | FB | 30% | 50% | 20% |
| [E.2] Errores del administrador | FB | 30% | 50% | 20% |
| [E.9] Errores de [re]-encaminamiento | FMB | 50% | | |
| [E.10] Errores de secuencia | FMB | | 50% | |
| [E.15] Alteración accidental de la información | FB | | 50% | |
| [E.18] Destrucción de la información | FMB | | | 20% |
| [E.19] Fugas de información | FB | | | 50% |
| [E.24] Caída del sistema por agotamiento de recursos | FM | | | 100% |
| [A.5] Suplantación de la identidad del usuario | FMB | 30% | 20% | 20% |
| [A.6] Abuso de privilegios de acceso | FMB | 30% | 20% | 20% |
| [A.7] Uso no previsto | FB | 30% | 50% | 50% |
| [A.9] [Re-]encaminamiento de mensajes | FMB | 50% | | |
| [A.10] Alteración de secuencia | FMB | | 50% | |
| [A.11] Acceso no autorizado | FMB | 60% | 50% | |
| [A.13] Repudio | FMB | | 50% | |

| | | | | |
|---|---|---|---|---|
| [A.15] Modificación deliberada de la información | FMB | | 50% | |
| [A.18] Destrucción de información | FMB | | | 50% |
| [A.19] Divulgación de información | FMB | 50% | | |
| [A.24] Denegación de servicio | FB | | | 100% |
| **[S] - SITIO WEB INSTITUCIONAL** | **FA** | **40%** | **45%** | **45%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.1] Errores de los usuarios | FB | 30% | 50% | 20% |
| [E.2] Errores del administrador | FB | 30% | 50% | 20% |
| [E.9] Errores de [re]-encaminamiento | FMB | 50% | | |
| [E.10] Errores de secuencia | FMB | | 50% | |
| [E.15] Alteración accidental de la información | FB | | 50% | |
| [E.18] Destrucción de la información | FMB | | | 20% |
| [E.19] Fugas de información | FB | | | 50% |
| [E.24] Caída del sistema por agotamiento de recursos | FM | | | 100% |
| [A.5] Suplantación de la identidad del usuario | FMB | 30% | 20% | 20% |
| [A.6] Abuso de privilegios de acceso | FMB | 30% | 20% | 20% |
| [A.7] Uso no previsto | FB | 30% | 50% | 50% |
| [A.9] [Re-]encaminamiento de mensajes | FMB | 50% | | |
| [A.10] Alteración de secuencia | FMB | | 50% | |
| [A.11] Acceso no autorizado | FMB | 60% | 50% | |
| [A.13] Repudio | FMB | | 50% | |
| [A.15] Modificación deliberada de la información | FMB | | 50% | |
| [A.18] Destrucción de información | FMB | | | 50% |
| [A.19] Divulgación de información | FMB | 50% | | |
| [A.24] Denegación de servicio | FB | | | 100% |
| **[S] - SWITCH TRANSACCIONALES. (INTERCAMBIO ELECTRÓNICO DE DATOS)** | **FA** | **40%** | **45%** | **45%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.1] Errores de los usuarios | FB | 30% | 50% | 20% |
| [E.2] Errores del administrador | FB | 30% | 50% | 20% |
| [E.9] Errores de [re]-encaminamiento | FMB | 50% | | |
| [E.10] Errores de secuencia | FMB | | 50% | |
| [E.15] Alteración accidental de la información | FB | | 50% | |
| [E.18] Destrucción de la información | FMB | | | 20% |
| [E.19] Fugas de información | FB | | | 50% |
| [E.24] Caída del sistema por agotamiento de recursos | FM | | | 100% |
| [A.5] Suplantación de la identidad del usuario | FMB | 30% | 20% | 20% |
| [A.6] Abuso de privilegios de acceso | FMB | 30% | 20% | 20% |
| [A.7] Uso no previsto | FB | 30% | 50% | 50% |
| [A.9] [Re-]encaminamiento de mensajes | FMB | 50% | | |
| [A.10] Alteración de secuencia | FMB | | 50% | |
| [A.11] Acceso no autorizado | FMB | 60% | 50% | |
| [A.13] Repudio | FMB | | 50% | |
| [A.15] Modificación deliberada de la información | FMB | | 50% | |
| [A.18] Destrucción de información | FMB | | | 50% |

| | | | | |
|---|---|---|---|---|
| [A.19] Divulgación de información | FMB | 50% | | |
| [A.24] Denegación de servicio | FB | | | 100% |
| **DATOS** | | | | |
| **[D] - DATOS DE CLIENTES (ABONADOS, FACTURACIÓN)** | **FB** | **70%** | **60%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.1] Errores de los usuarios | FM | 100% | 50% | 100% |
| [E.2] Errores del administrador | FMB | 100% | 50% | 100% |
| [E.15] Alteración accidental de la información | FM | | 50% | |
| [E.18] Destrucción de información | FB | | | 100% |
| [E.19] Fugas de información | FMB | 50% | | |
| [A.5] Suplantación de la identidad del usuario | FMB | 50% | 100% | 100% |
| [A.6] Abuso de privilegios de acceso | FM | 50% | 50% | 100% |
| [A.11] Acceso no autorizado | FM | 60% | 60% | |
| [A.14] Interceptación de información (escucha) | FMB | 50% | | |
| [A.15] Modificación deliberada de la información | FB | | 60% | |
| [A.18] Destrucción de información | FMB | | | 100% |
| [A.19] Divulgación de información | FA | 100% | | |
| **[D] - DATOS DE GESTIÓN INTERNA** | **FB** | **70%** | **60%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.1] Errores de los usuarios | FM | 100% | 50% | 100% |
| [E.2] Errores del administrador | FMB | 100% | 50% | 100% |
| [E.15] Alteración accidental de la información | FM | | 50% | |
| [E.18] Destrucción de información | FB | | | 100% |
| [E.19] Fugas de información | FMB | 50% | | |
| [A.5] Suplantación de la identidad del usuario | FMB | 50% | 100% | 100% |
| [A.6] Abuso de privilegios de acceso | FM | 50% | 50% | 100% |
| [A.11] Acceso no autorizado | FM | 60% | 60% | |
| [A.14] Interceptación de información (escucha) | FMB | 50% | | |
| [A.15] Modificación deliberada de la información | FB | | 60% | |
| [A.18] Destrucción de información | FMB | | | 100% |
| [A.19] Divulgación de información | FA | 100% | | |
| **[D] - DATOS FINANCIEROS - CONTABLES** | **FB** | **70%** | **60%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.1] Errores de los usuarios | FM | 100% | 50% | 100% |
| [E.2] Errores del administrador | FMB | 100% | 50% | 100% |
| [E.15] Alteración accidental de la información | FM | | 50% | |
| [E.18] Destrucción de información | FB | | | 100% |
| [E.19] Fugas de información | FMB | 50% | | |
| [A.5] Suplantación de la identidad del usuario | FMB | 50% | 100% | 100% |
| [A.6] Abuso de privilegios de acceso | FM | 50% | 50% | 100% |
| [A.11] Acceso no autorizado | FM | 60% | 60% | |
| [A.14] Interceptación de información (escucha) | FMB | 50% | | |
| [A.15] Modificación deliberada de la información | FB | | 60% | |
| [A.18] Destrucción de información | FMB | | | 100% |
| [A.19] Divulgación de información | FA | 100% | | |

| [D] - INFORMACIÓN DE USUARIOS | FB | 20% | 10% | 15% |
|---|---|---|---|---|
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.1] Errores de los usuarios | FM | 20% | 20% | 20% |
| [E.2] Errores del administrador | FB | 20% | 10% | 20% |
| [E.15] Alteración accidental de la información | FB | | 10% | |
| [E.18] Destrucción de información | FM | | | 20% |
| [E.19] Fugas de información | FM | 50% | | |
| [A.5] Suplantación de la identidad del usuario | FMB | 10% | 5% | 10% |
| [A.6] Abuso de privilegios de acceso | FB | 10% | 5% | 10% |
| [A.11] Acceso no autorizado | FB | 20% | 10% | |
| [A.14] Interceptación de información (escucha) | FMB | 20% | | |
| [A.15] Modificación deliberada de la información | FMB | | 10% | |
| [A.18] Destrucción de información | FMB | | | 10% |
| [A.19] Divulgación de información | FMB | 10% | | |
| **[D] - REGISTROS DE ACTIVIDAD (LOGS)** | **FB** | **70%** | **60%** | **100%** |
| **LISTA DE AMENAZAS** | **FREC** | **C** | **I** | **D** |
| [E.1] Errores de los usuarios | FM | 100% | 50% | 100% |
| [E.2] Errores del administrador | FMB | 100% | 50% | 100% |
| [E.15] Alteración accidental de la información | FM | | 50% | |
| [E.18] Destrucción de información | FB | | | 100% |
| [E.19] Fugas de información | FMB | 50% | | |
| [A.5] Suplantación de la identidad del usuario | FMB | 50% | 100% | 100% |
| [A.6] Abuso de privilegios de acceso | FM | 50% | 50% | 100% |
| [A.11] Acceso no autorizado | FM | 60% | 60% | |
| [A.14] Interceptación de información (escucha) | FMB | 50% | | |
| [A.15] Modificación deliberada de la información | FB | | 60% | |
| [A.18] Destrucción de información | FMB | | | 100% |
| [A.19] Divulgación de información | FA | 100% | | |

*Tabla 15 - Activo VS Amenaza.*

## 3.4 Cálculo Del Impacto Potencial.

Habiendo llegado a este punto es necesario determinar el impacto potencial que no es más que el daño sobre el activo derivado de la materialización de la amenaza.
Este cálculo resulta indispensable ya será nuestra guía al momento de priorizar los proyectos a establecer y el plan de acción a ejecutar.

A continuación en la siguiente tabla realizamos el cálculo:

**Impacto = Valor del activo x Porcentaje de impacto.**

| AMBITO | ACTIVO | CRITICIDAD | | | %IMPACTO | | | IMPACTO POTENCIAL | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | C | I | D | C | I | D | C | I | D |
| **Hardware [HW]** | AACC de precisión. | 4 | 8 | 10 | 35% | 50% | 100% | **1,4** | **4,0** | **10,0** |
| | Cableado estructurado. | 8 | 8 | 8 | 55% | 50% | 100% | **4,4** | **4,0** | **8,0** |
| | CCTV (video vigilancia). | 8 | 8 | 8 | 35% | 30% | 100% | **2,8** | **2,4** | **8,0** |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Dispositivos biométricos. (Acceso y Asistencia) | 8 | 6 | 8 | 45% | 35% | 100% | **3,6** | **2,1** | **8,0** |
| | Dispositivos telefónicos. | 6 | 6 | 8 | 50% | 40% | 100% | **3,0** | **2,4** | **8,0** |
| | Equipos de red. (ACCESS POINT, SWITCH) | 10 | 10 | 8 | 50% | 35% | 100% | **5,0** | **3,5** | **8,0** |
| | Estaciones de trabajo. | 6 | 6 | 6 | 50% | 50% | 100% | **3,0** | **3,0** | **6,0** |
| | Firewalls. | 10 | 8 | 10 | 50% | 25% | 100% | **5,0** | **2,0** | **10,0** |
| | Impresoras. | 4 | 2 | 4 | 50% | 50% | 100% | **2,0** | **1,0** | **4,0** |
| | Routers. | 6 | 6 | 10 | 55% | 25% | 100% | **3,3** | **1,5** | **10,0** |
| | Servidor de archivos. (NAS) | 8 | 6 | 8 | 100% | 80% | 100% | **8,0** | **4,8** | **8,0** |
| | Servidor de correo electrónico. | 8 | 6 | 8 | 95% | 80% | 100% | **7,6** | **4,8** | **8,0** |
| | Servidor de telefonía IP. | 2 | 8 | 10 | 90% | 80% | 100% | **1,8** | **6,4** | **10,0** |
| | Servidor Georreferenciación. (GIS) | 8 | 6 | 8 | 90% | 80% | 100% | **7,2** | **4,8** | **8,0** |
| | Servidores de autómatas (SCADA). | 10 | 8 | 10 | 90% | 80% | 100% | **9,0** | **6,4** | **10,0** |
| | Servidores de virtualización. | 10 | 8 | 10 | 90% | 80% | 100% | **9,0** | **6,4** | **10,0** |
| | UPS | 4 | 8 | 10 | 90% | 80% | 100% | **3,6** | **6,4** | **10,0** |
| Software [SW] | Antivirus. | 2 | 8 | 8 | 85% | 100% | 100% | **1,7** | **8,0** | **8,0** |
| | Aplicaciones internas. | 2 | 8 | 10 | 90% | 100% | 100% | **1,8** | **8,0** | **10,0** |
| | Herramientas de desarrollo . | 10 | 8 | 8 | 90% | 100% | 100% | **9,0** | **8,0** | **8,0** |
| | Programas utilitarios. | 2 | 8 | 6 | 90% | 90% | 100% | **1,8** | **7,2** | **6,0** |
| | Sistemas operativos. | 2 | 2 | 2 | 90% | 90% | 100% | **1,8** | **1,8** | **2,0** |
| | Software de Correo electrónico. | 10 | 8 | 8 | 85% | 100% | 100% | **8,5** | **8,0** | **8,0** |
| | Software de virtualización. | 10 | 8 | 8 | 85% | 100% | 100% | **8,5** | **8,0** | **8,0** |
| | Software SCADA. | 6 | 8 | 10 | 85% | 100% | 100% | **5,1** | **8,0** | **10,0** |
| **PERSONAL [P]** | Alta Gerencia (Toma de decisiones). | 2 | 8 | 8 | 60% | 50% | 55% | **1,2** | **4,0** | **4,4** |
| | Control de Accesos. (Guardianía) | 2 | 8 | 10 | 50% | 30% | 30% | **1,0** | **2,4** | **3,0** |
| | Desarrolladores de software. | 10 | 8 | 8 | 100% | 50% | 75% | **10,0** | **4,0** | **6,0** |
| | Personal externo. (proveedores, contratistas). | 2 | 8 | 6 | 50% | 30% | 30% | **1,0** | **2,4** | **1,8** |
| | Personal operativo (personal obrero/limpieza). | 2 | 2 | 2 | 50% | 30% | 30% | **1,0** | **0,6** | **0,6** |
| | Personal tecnológico (infraestructura - soporte). | 10 | 8 | 8 | 100% | 50% | 75% | **10,0** | **4,0** | **6,0** |
| | Usuarios finales. (personal administrativo). | 10 | 8 | 8 | 50% | 30% | 30% | **5,0** | **2,4** | **2,4** |
| Instalaciones [L] | Centros de Datos. | 2 | 8 | 10 | 60% | 55% | 100% | **1,2** | **4,4** | **10,0** |
| | Centro de Monitoreo (Sala de Control SCADA). | 2 | 8 | 10 | 60% | 55% | 100% | **1,2** | **4,4** | **10,0** |
| | Instalaciones estructurales. (Edificio, estaciones). | 2 | 8 | 10 | 60% | 55% | 100% | **1,2** | **4,4** | **10,0** |
| | Laboratorios de Agua Potable. | 2 | 6 | 6 | 60% | 55% | 100% | **1,2** | **3,3** | **6,0** |
| | Plantas de bombeo y tratamiento. | 2 | 8 | 6 | 60% | 55% | 100% | **1,2** | **4,4** | **6,0** |
| **Servicios [S]** | Correo electrónico. | 8 | 6 | 8 | 70% | 70% | 90% | **5,6** | **4,2** | **7,2** |
| | Infraestructura cloud. | 10 | 6 | 10 | 40% | 45% | 45% | **4,0** | **2,7** | **4,5** |
| | Portales tecnológicos publicados. | 10 | 6 | 10 | 40% | 45% | 45% | **4,0** | **2,7** | **4,5** |
| | Sitio Web institucional. | 8 | 6 | 8 | 40% | 45% | 45% | **3,2** | **2,7** | **3,6** |
| | SWITCH transaccionales. (intercambio electrónico de datos) | 10 | 10 | 10 | 40% | 45% | 45% | **4,0** | **4,5** | **4,5** |
| Datos. [D] | Datos de clientes (abonados). | 8 | 10 | 10 | 70% | 60% | 100% | **5,6** | **6,0** | **10,0** |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Datos de gestión interna. | 6 | 8 | 10 | 70% | 60% | 100% | **4,2** | **4,8** | **10,0** |
| | Datos financieros - contables. | 8 | 10 | 10 | 70% | 60% | 100% | **5,6** | **6,0** | **10,0** |
| | Información de usuarios (personal). | 2 | 2 | 2 | 20% | 10% | 15% | **0,4** | **0,2** | **0,3** |
| | Registros de actividad (logs). | 8 | 8 | 10 | 70% | 60% | 100% | **5,6** | **4,8** | **10,0** |

*Tabla 16 - Cálculo Impacto Potencial.*

### 3.5 Cálculo Del Riesgo.

Posterior a calcular el impacto potencial ahora contamos con un insumo necesario para poder calcular el riesgo potencial asociado , basado en la frecuencia que pueda tener la ocurrencia de las amenazas proyectadas y su valor numérico.

La fórmula sería: **Riesgo = Frecuencia x Impacto.**

| AMBITO | ACTIVO | FRECUENCIA | | IMPACTO POTENCIAL | | | RIESGO POTENCIAL | | |
|---|---|---|---|---|---|---|---|---|---|
| | | FREC | VAL | C | I | D | C | I | D |
| **Hardware [HW]** | AACC de precisión. | **FA** | **10** | 1,4 | 4,0 | 10,0 | **14,00** | **40,00** | **100** |
| | Cableado estructurado. | **FMB** | **0,01** | 4,4 | 4,0 | 8,0 | **0,04** | **0,04** | **0,08** |
| | CCTV (video vigilancia). | **FMB** | **0,01** | 2,8 | 2,4 | 8,0 | **0,03** | **0,02** | **0,08** |
| | Dispositivos biométricos. (Acceso y Asistencia) | **FM** | **1** | 3,6 | 2,1 | 8,0 | **3,60** | **2,10** | **8,00** |
| | Dispositivos telefónicos. | **FMB** | **0,01** | 3,0 | 2,4 | 8,0 | **0,03** | **0,02** | **0,08** |
| | Equipos de red. (ACCESS POINT, SWITCH) | **FB** | **0,1** | 5,0 | 3,5 | 8,0 | **0,50** | **0,35** | **0,80** |
| | Estaciones de trabajo. | **FM** | **1** | 3,0 | 3,0 | 6,0 | **3,00** | **3,00** | **6,00** |
| | Firewalls. | **FM** | **1** | 5,0 | 2,0 | 10,0 | **5,00** | **2,00** | **10,00** |
| | Impresoras. | **FMB** | **1** | 2,0 | 1,0 | 4,0 | **2,00** | **1,00** | **4,00** |
| | Routers. | **FB** | **0,1** | 3,3 | 1,5 | 10,0 | **0,33** | **0,15** | **1,00** |
| | Servidor de archivos. (NAS) | **FA** | **10** | 8,0 | 4,8 | 8,0 | **80,00** | **48,00** | **80,00** |
| | Servidor de correo electrónico. | **FA** | **10** | 7,6 | 4,8 | 8,0 | **76,00** | **48,00** | **80,00** |
| | Servidor de telefonía IP. | **FMB** | **1** | 1,8 | 6,4 | 10,0 | **1,80** | **6,40** | **10,00** |
| | Servidor Georreferenciación. (GIS) | **FB** | **0,1** | 7,2 | 4,8 | 8,0 | **0,72** | **0,48** | **0,80** |
| | Servidores de autómatas (SCADA). | **FB** | **0,1** | 9,0 | 6,4 | 10,0 | **0,90** | **0,64** | **1,00** |
| | Servidores de virtualización. | **FB** | **0,1** | 9,0 | 6,4 | 10,0 | **0,90** | **0,64** | **1,00** |
| | UPS | **FA** | **10** | 3,6 | 6,4 | 10,0 | **36,00** | **64,00** | **100** |
| Software [SW] | Antivirus. | **FA** | **10** | 1,7 | 8,0 | 8,0 | **16,92** | **80,00** | **80,00** |
| | Aplicaciones internas. | **FA** | **10** | 1,8 | 8,0 | 10,0 | **18,08** | **80,00** | **100** |
| | Herramientas de desarrollo . | **FA** | **10** | 9,0 | 8,0 | 8,0 | **90,38** | **80,00** | **80,00** |
| | Programas utilitarios. | **FA** | **10** | 1,8 | 7,2 | 6,0 | **18,08** | **72,27** | **60,00** |
| | Sistemas operativos. | **FM** | **1** | 1,8 | 1,8 | 2,0 | **1,81** | **1,81** | **2,00** |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Software de Correo electrónico. | **FM** | **1** | 8,5 | 8,0 | 8,0 | **8,46** | **8,00** | **8,00** |
| | Software de virtualización. | **FM** | **1** | 8,5 | 8,0 | 8,0 | **8,46** | **8,00** | **8,00** |
| | Software SCADA. | **FB** | **0,1** | 5,1 | 8,0 | 10,0 | **0,51** | **0,80** | **1,00** |
| **PERSONAL [P]** | Alta Gerencia (Toma de decisiones). | **FM** | **1** | 1,2 | 4,0 | 4,4 | **1,20** | **4,00** | **4,40** |
| | Control de Accesos. (Guardianía) | **FM** | **1** | 1,0 | 2,4 | 3,0 | **1,00** | **2,40** | **3,00** |
| | Desarrolladores de software. | **FA** | **10** | 10,0 | 4,0 | 6,0 | **100** | **40,00** | **60,00** |
| | Personal externo. (proveedores, contratistas). | **FM** | **1** | 1,0 | 2,4 | 1,8 | **1,00** | **2,40** | **1,80** |
| | Personal operativo (personal obrero/limpieza). | **FM** | **1** | 1,0 | 0,6 | 0,6 | **1,00** | **0,60** | **0,60** |
| | Personal tecnológico (infraestructura - soporte). | **FA** | **10** | 10,0 | 4,0 | 6,0 | **100** | **40,00** | **60,00** |
| | Usuarios finales. (personal administrativo). | **FA** | **10** | 5,0 | 2,4 | 2,4 | **50,00** | **24,00** | **24,00** |
| Instalaciones [L] | Centros de Datos. | **FM** | **1** | 1,2 | 4,4 | 10,0 | **1,20** | **4,40** | **10,00** |
| | Centro de Monitoreo (Sala de Control SCADA). | **FM** | **1** | 1,2 | 4,4 | 10,0 | **1,20** | **4,40** | **10,00** |
| | Instalaciones estructurales. (Edificio, estaciones). | **FB** | **0,1** | 1,2 | 4,4 | 10,0 | **0,12** | **0,44** | **1,00** |
| | Laboratorios de Agua Potable. | **FB** | **0,1** | 1,2 | 3,3 | 6,0 | **0,12** | **0,33** | **0,60** |
| | Plantas de bombeo y tratamiento. | **FB** | **0,1** | 1,2 | 4,4 | 6,0 | **0,12** | **0,44** | **0,60** |
| **Servicios [S]** | Correo electrónico. | **FA** | **10** | 5,6 | 4,2 | 7,2 | **56,00** | **42,00** | **72,00** |
| | Infraestructura cloud. | **FA** | **10** | 4,0 | 2,7 | 4,5 | **40,00** | **26,73** | **45,00** |
| | Portales tecnológicos publicados. | **FA** | **10** | 4,0 | 2,7 | 4,5 | **40,00** | **26,73** | **45,00** |
| | Sitio Web institucional. | **FA** | **10** | 3,2 | 2,7 | 3,6 | **32,00** | **26,73** | **36,00** |
| | SWITCH transaccionales. (intercambio electrónico de datos) | **FA** | **10** | 4,0 | 4,5 | 4,5 | **40,00** | **44,55** | **45,00** |
| Datos. [D] | Datos de clientes (abonados). | **FB** | **0,1** | 5,6 | 6,0 | 10,0 | **0,56** | **0,60** | **1,00** |
| | Datos de gestión interna. | **FB** | **0,1** | 4,2 | 4,8 | 10,0 | **0,42** | **0,48** | **1,00** |
| | Datos financieros - contables. | **FB** | **0,1** | 5,6 | 6,0 | 10,0 | **0,56** | **0,60** | **1,00** |
| | Información de usuarios (personal). | **FB** | **0,1** | 0,4 | 0,2 | 0,3 | **0,04** | **0,02** | **0,03** |
| | Registros de actividad (logs). | **FB** | **0,1** | 5,6 | 4,8 | 10,0 | **0,56** | **0,48** | **1,00** |

RIESGO NO ACEPTABLE

RIESGO ACEPTABLE

*Tabla 17 - Cálculo de Riesgo Potencial.*

## 3.6 Resultados.

Como insumos finales de esta sección hemos de resaltar que hemos conseguido evidenciar:

- El riesgo potencial evaluado.
- Los activos que enfrentan mayores amenazas en un entorno con frecuencias medias y altas.
- Hemos definido el riesgo aceptable y el no aceptable, el cual está por encima de los 40 puntos , esto nos indica que las mejoras en estos rubros deben ser inmediatas.

# 4. Propuestas de proyectos.

## 4.1 Introducción.

El análisis de riesgos realizado en la sección anterior es el disparador y punto de origen para el despliegue nuestros proyectos que forman parte de la propuesta.

El riesgo potencial asociado a cada activo nos provee un panorama más claro acerca de los puntos débiles de la organización en temas de seguridad de la información. Los proyectos que se presentan a continuación tratan de una serie de acciones conjuntas que pretenden controlar el riesgo para que sus índices se reduzcan considerablemente y mantengan los activos un nivel por debajo del riesgo aceptable.

## 4.2 Propuesta.

Los proyectos propuestos son cuatro:

- **Proyecto 1 (PR1) .-** Proyecto para aseguramiento de las operaciones y continuidad del negocio.
- **Proyecto 2 (PR2) .-** Proyecto estandarización de usuarios y contraseña.
- **Proyecto 3 (PR3) .-** Revisión y calificación de servicios que involucren intercambio de datos.
- **Proyecto 4 (PR4) .-** Proyecto Licenciamiento de software propietario / uso de software libre.

| PROYECTO 1: ASEGURAMIENTO DE LAS OPERACIONES Y CONTINUIDAD DEL NEGOCIO. | |
|---|---|
| **EQUIPO** | Oficial de Seguridad , Gerente de TI , Responsable de Mantenimiento Eléctrico. |
| **OBJETIVO** | Documentar procedimientos que soporten la implementación de controles que respalden la política de seguridad propuesta. |
| **ACTIVIDADES** | Definición de un Plan de respaldo de datos sensibles almacenados en infraestructura. |
| | Crear un esquema de continuidad de negocio y recuperación ante desastres. |
| | Tomar acciones respecto al respaldo de suministro eléctrico. |
| | Definir planes de mantenimiento para climatización de centro de datos y cuartos de equipos |
| | Definir políticas de accesos a áreas restringidas. |
| **BENEFICIO** | Contar con el mayor porcentaje de horas de servicios tecnológicos ininterrumpidas. |
| | Aseguramiento y protección de los datos de la organización. |
| **RIESGO A MITIGAR** | [HW] AACC de precisión - [HW] UPS - [HW] NAS - [HW] SERVIDOR CORREO ELECTRÓNICO. |
| | CONTROLES: A.11.1 - A.17.1 - A.17.2 |
| **INICIO** | 1/7/21 |
| **DURACIÓN** | 6 SEMANAS |
| **FIN** | 12/8/21 |
| **PRESUPUESTO** | $2.000,00 |

| PROYECTO 2: ESTANDARIZACIÓN DE USUARIOS Y CONTRASEÑAS. | |
|---|---|
| **EQUIPO** | Oficial de Seguridad , Gerente de TI, Gerente de TTHH. |
| **OBJETIVO** | Documentar procedimientos que soporten la implementación de controles que respalden la política de usuarios y contraseñas. |
| **ACTIVIDADES** | Socializar política de usuarios y contraseñas. |
| | Expedición de acuerdo de confidencialidad y uso de medios electrónicos. |
| | Definición de umbrales y directivas de seguridad para autenticación de usuarios. |
| | Definición de un plan de inducción/capacitación para usuarios finales y personal de nuevo ingreso, concerniente a responsabilidad y buen uso de usuarios y contraseñas. |
| **BENEFICIO** | Contar con perfiles individuales para el uso de estaciones de trabajo y sistemas de información. |
| | Minimizar el riesgo del uso de usuarios genéricos , anónimos , privilegios inadecuados y accesos no autorizados a equipos y sistemas de información. |
| **RIESGO A MITIGAR** | [P] Desarrolladores de Software - [P] Tecnológico Infraestructura - [P] Usuarios finales - [SW] Aplicaciones Internas. |
| | CONTROLES: A.9.2 - A.9.3 - A.9.4 - A.18.1 - A.18.2 |
| **INICIO** | 15/8/21 |
| **DURACIÓN** | 8 SEMANAS |
| **FIN** | 10/10/21 |
| **PRESUPUESTO** | $1.000,00 |

| PROYECTO 3: REVISIÓN Y CALIFICACIÓN DE SERVICIOS QUE INVOLUCREN INTERCAMBIO DE DATOS. | |
|---|---|
| **EQUIPO** | Oficial de Seguridad , Gerente de TI. |
| **OBJETIVO** | Establecer un esquema para calificación de requisitos de seguridad de información para servicios internos o externos que involucren intercambio de datos. |
| **ACTIVIDADES** | Definición de requisitos mínimos de seguridad para servicios tecnológicos antes de su adquisición o publicación. |
| | Realizar inventario de puertos necesarios que utilicen los servicios. |
| | Definir privilegios mínimos durante las etapas de testeo de los servicios. |
| | Documentar plan de reverso (roll-back) por cada nueva implementación, antes de la etapa de producción o publicación. |
| **BENEFICIO** | Proteger la infraestructura tecnológica de la organización frente a ataques o acciones fraudulentas. |
| | Aseguramiento y protección de los datos de la organización. |
| **RIESGO A MITIGAR** | [S] Correo electrónico - [S] Infraestructura Cloud - [S] Portales Publicados - [S] SWITCH transaccionales (Middleware) |
| | CONTROLES: A.14.1 - A.14.2 - A14.3 - A.12.6 |
| **INICIO** | 1/12/21 |
| **DURACIÓN** | 6 SEMANAS |
| **FIN** | 12/1/22 |
| **PRESUPUESTO** | $1.000,00 |

| PROYECTO 4: LICENCIAMIENTO DE SOFTWARE PROPIETARIOS / USO DE SOFTWARE LIBRE. | |
|---|---|
| **EQUIPO** | Oficial de Seguridad , Gerente de TI , Gerente de Compras. |
| **OBJETIVO** | Contar con software utilitario licenciado. |

| | |
|---|---|
| **ACTIVIDADES** | Realizar un inventario de software necesario para las actividades de la organización. |
| | Realizar un análisis de alternativas para solventar las necesidades mediante software libre. |
| | Definir un procedimiento de revisión de equipos ajenos a la organización antes de concederles acceso a la red de datos institucional. |
| | Eliminar de las estaciones de trabajo cracks y parches con código malicioso que simulen licenciamiento. |
| | Definición de un plan de inducción/capacitación para usuarios finales acerca de herramientas ofimáticas de software libre. |
| **BENEFICIO** | Contar con software legalmente reconocido y funcional. |
| | Minimizar el riesgo de malware, virus y código malicioso que pongan en riesgo la infraestructura tecnológica de la organización. |
| **RIESGO A MITIGAR** | [SW] Antivirus. - [SW] Herramientas Desarrollo de Software. - [SW] Programas Utilitarios. |
| | CONTROLES: A.11.1 - A.11.2 - A.12.2 |
| **INICIO** | 15/10/21 |
| **DURACIÓN** | 8 SEMANAS |
| **FIN** | 10/12/21 |
| **PRESUPUESTO** | $5.000,00 |

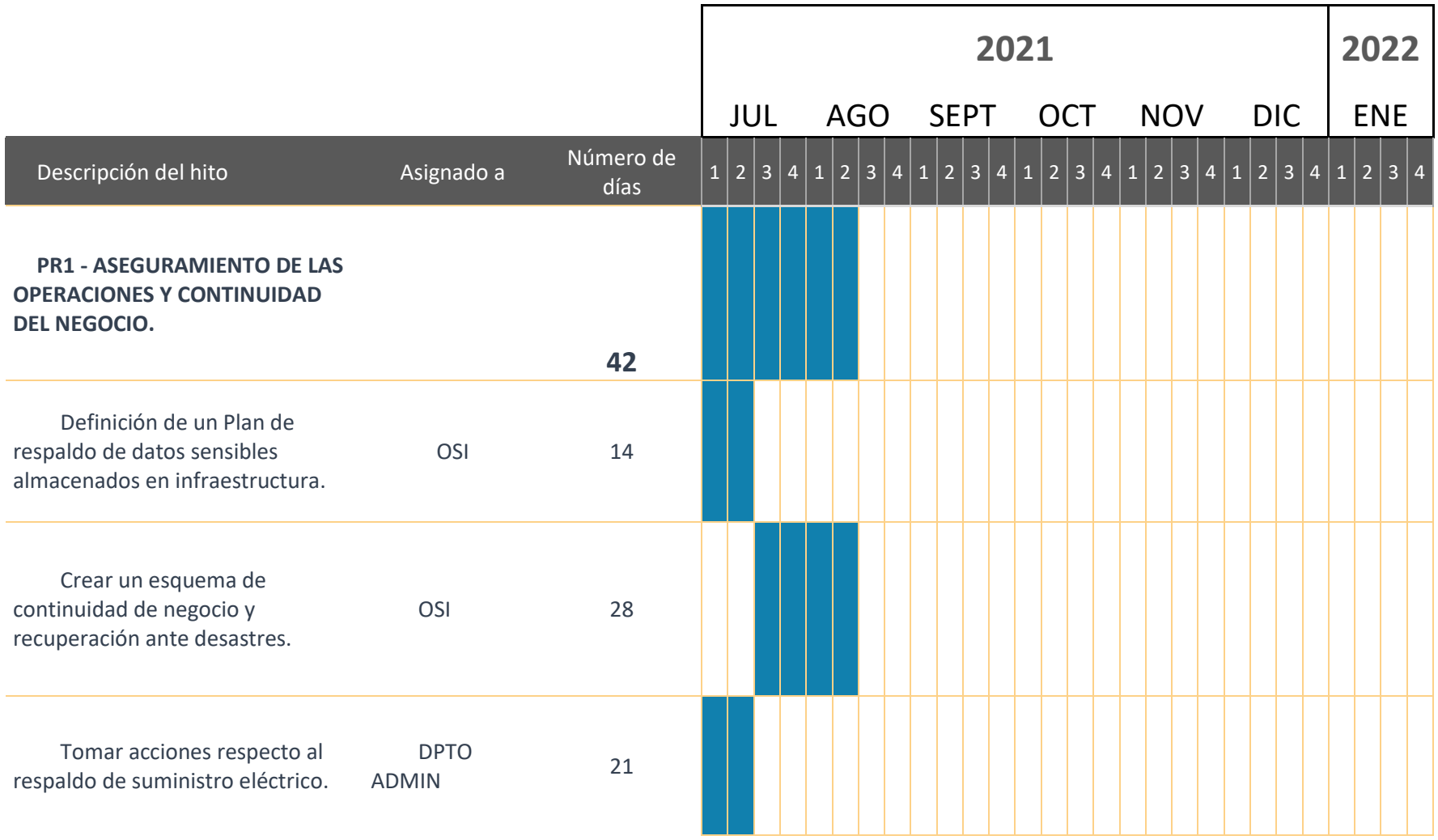
*Tabla 18 - Propuesta de Proyectos.*

## 4.3 Planificación.

Para la comprensión de el despliegue de los proyectos establecemos el siguiente diagrama de Gantt con la intención de resumir el desarrollo programado de los proyectos en el lapso de meses desde Julio 2021 a Enero 2022.

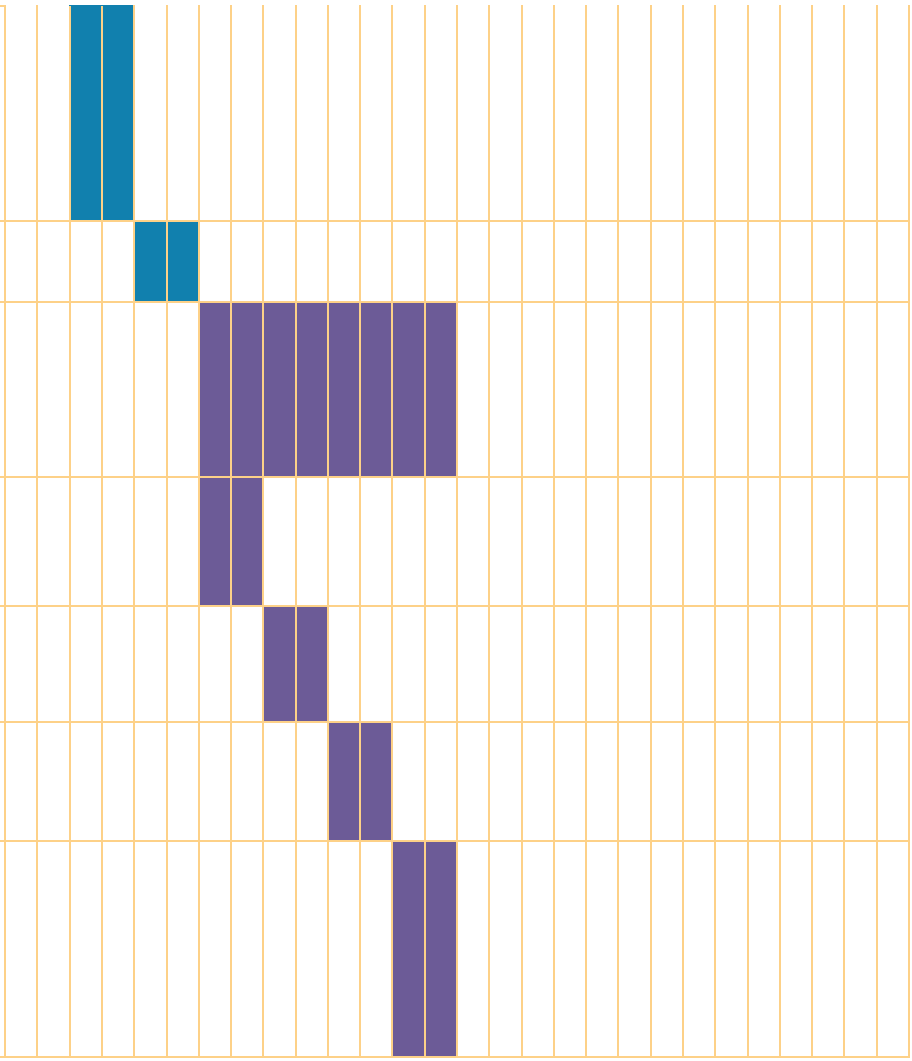
La siguiente tabla detalla actividades a realizar , los responsables de las mismas y el número de días contemplados para el desarrollo de estas.

## PLANIFICACIÓN PROPUESTAS DE PROYECTOS

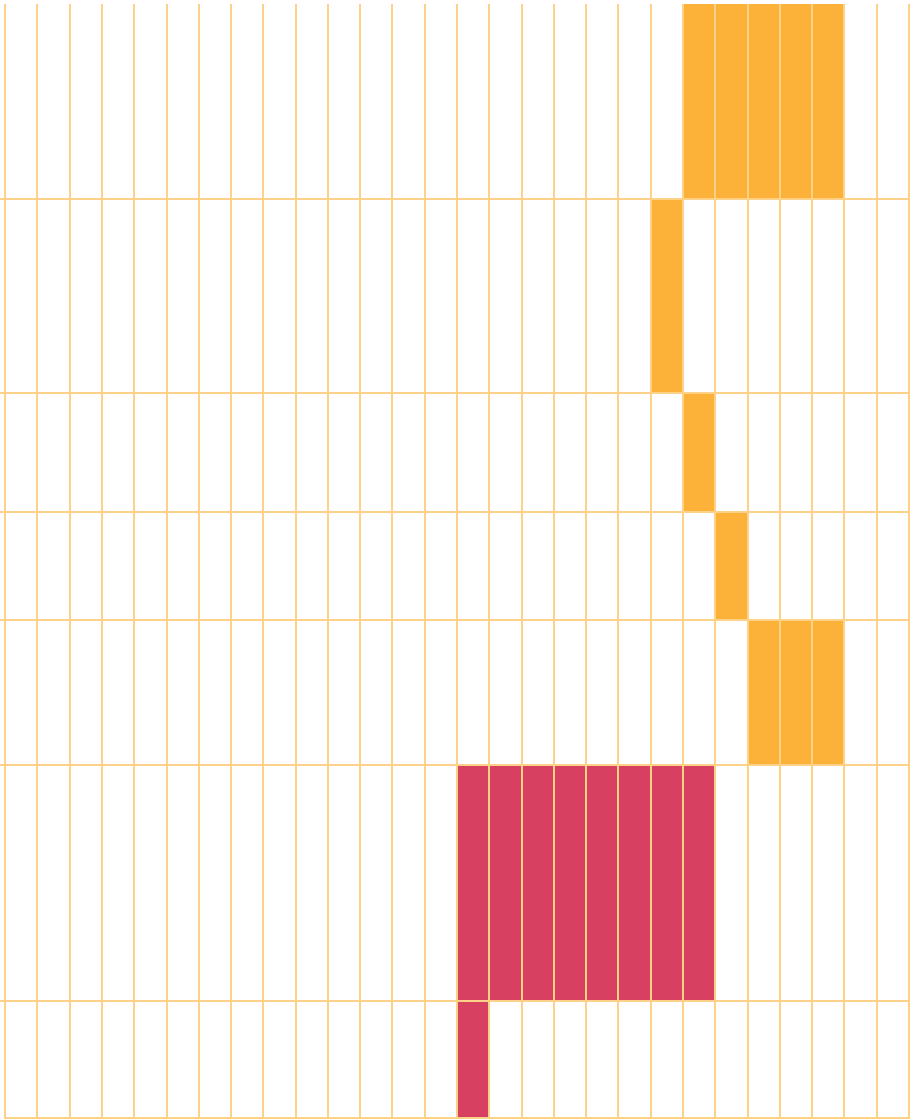


| Descripción del hito | Asignado a | Número de días |
|---|---|---|
| **PR1 - ASEGURAMIENTO DE LAS OPERACIONES Y CONTINUIDAD DEL NEGOCIO.** | | **42** |
| Definición de un Plan de respaldo de datos sensibles almacenados en infraestructura. | OSI | 14 |
| Crear un esquema de continuidad de negocio y recuperación ante desastres. | OSI | 28 |
| Tomar acciones respecto al respaldo de suministro eléctrico. | DPTO ADMIN | 21 |

| | | |
|---|---|---|
| Definir planes de mantenimiento para climatización de centro de datos y cuartos de equipos | DPTO ADMIN | 21 |
| Definir políticas de accesos a áreas restringidas. | DPTO ADMIN | 21 |
| **PR2 -ESTANDARIZACIÓN DE USUARIOS Y CONTRASEÑAS.** | | **56** |
| Socializar política de usuarios y contraseñas. | OSI | 14 |
| Expedición de acuerdo de confidencialidad y uso de medios electrónicos. | TTHH | 14 |
| Definición de umbrales y directivas de seguridad para autenticación de usuarios. | GTI | 14 |
| Definición de un plan de inducción/capacitación para usuarios finales y personal de nuevo ingreso, concerniente a responsabilidad y buen uso de usuarios y contraseñas. | TTHH | 14 |



| | | |
|---|---|---|
| **PR3 - REVISIÓN Y CALIFICACIÓN DE SERVICIOS QUE INVOLUCREN INTERCAMBIO DE DATOS.** | | **42** |
| Definición de requisitos mínimos de seguridad para servicios tecnológicos antes de su adquisición o publicación. | OSI | 7 |
| Realizar inventario de puertos necesarios que utilicen los servicios. | OSI | 7 |
| Definir privilegios mínimos durante las etapas de testeo de los servicios. | GTI | 7 |
| Documentar plan de reverso (roll-back) por cada nueva implementación, antes de la etapa de producción o publicación. | GTI | 21 |
| **PR4 - LICENCIAMIENTO DE SOFTWARE PROPIETARIOS / USO DE SOFTWARE LIBRE.** | | **56** |
| Realizar un inventario de software necesario para las actividades de la organización. | OSI | 7 |



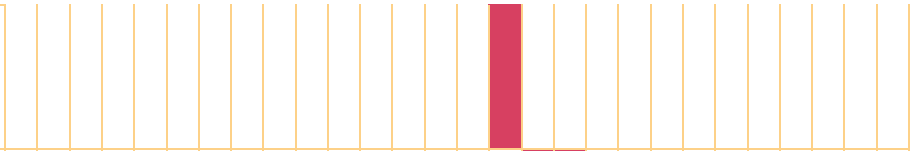
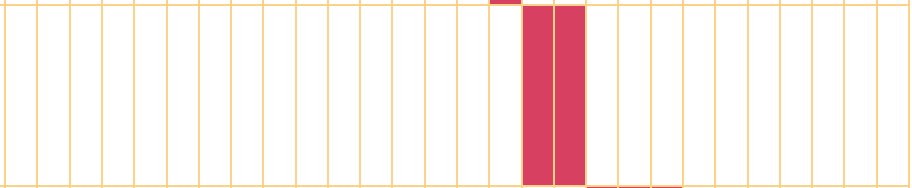
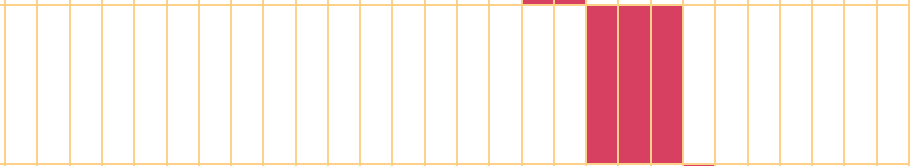
| | | | |
|---|---|---|---|
| Realizar un análisis de alternativas para solventar las necesidades mediante software libre. | OSI | 7 |  |
| Definir un procedimiento de revisión de equipos ajenos a la organización antes de concederles acceso a la red de datos institucional. | DPTO ADMIN | 14 |  |
| Eliminar de las estaciones de trabajo cracks y parches con código malicioso que simulen licenciamiento. | DPTO ADMIN | 21 |  |
| Definición de un plan de inducción/capacitación para usuarios finales acerca de herramientas ofimáticas de software libre. | DPTO ADMIN | 7 |  |

*Tabla 19 - Planificación Proyectos*

# 5. Auditoría de cumplimiento.

## 5.1 Introducción.

Ahora que conocemos los activos y hemos efectuado la evaluación de amenazas y calculado el impacto y su riesgo es preciso analizar el cumplimiento de la organización respecto a las buenas prácticas en el ámbito de la seguridad de la información.
Nuestra principal guía será la ISO/IEC 27002:2013, esta norma será nuestra plantilla para la evaluación de la organización frente al marco de control que nos llevará a la situación deseada.

## 5.2 Metodología.

Los 114 controles mencionados varias veces en este documento pertencen al estándar ISO/IEC 27002:2013, nos proporcionan un modelo para el establecimiento y posicionamiento de la seguridad de la información; enmarcando estos rubros en 14 dominios y 35 objetivos de controles. El reconocimiento internacional con el que cuenta esta norma la hacen más que idónea para ser aplicado en la mayoría de las organizaciones.

Siguiendo nuestro procedimiento de auditoria desarrollado en el punto 2.2.2 seguimos las directrices exponiendo adjunto al plan indicado
La aplicabilidad de esta norma en nuestro Plan director para esta fase de auditorias de cumplimiento será regida por el modelo de de madurez de la capacidad (CMM), con el cual evaluaremos el grado de efectividad bajo ciertas variables.
Para la comprensión de este modelo desplegamos el siguiente cuadro donde detallamos lo mencioando con antelación.

| EFECTIVIDAD | CMM | SIGNIFICADO | DESCRIPCIÓN |
|---|---|---|---|
| 0% | L0 | Inexistente | No existen registros acerca de procesos reconocibles ni problema a resolver. |
| 10% | L1 | Inicial/Ad- hoc | Estado inicial , procesos manuales o procesos basados en esfuerzo humano. No existe documentación ni flujos establecidos para el cumplimiento de los procesos. |
| 50% | L2 | Repetible pero intuitivo | Procesos realizados por intuición pero sin documentar del todo , muchas veces basados en experiencias o métodos empíricos . No existe entrenamiento formal ni comunicación oficial, las responsabilidades quedan a |

| | | | |
|---|---|---|---|
| | | | cargo de cada individuo. Se depende del grado de conocimiento del personal. |
| 90% | L3 | Proceso definido | La mayoría del personal de organización participa en el proceso. Los procesos están implantados, documentados y los responsables han sido capacitados. |
| 95% | L4 | Gestionado y Medible | Procesos maduros que pueden ser medidos bajo indicadores de cumplimiento, son objeto de seguimiento y evaluación. Cuenta con tecnología para automatizar el flujo de trabajo y mejorar la calidad y la eficiencia. |
| 100% | L5 | Optimizado | Procesos inmersos en constante mejora continua, bajo modelos matemáticos se determinan las desviaciones más comunes y se optimizan los procesos. |

*Tabla 20 - Modelo CMM Capacidad de Madurez.*

## 5.3 Evaluación De La Madurez.

Esta fase está dedicada a evaluar los diferentes dominios de control y los 114 controles planteados por la ISO/IEC27002:2013. Esta auditoría se lleva a cabo partiendo de que todos los proyectos propuestos en la sección 4 de este plan han sido ejecutados correctamente.

De forma resumida, los dominios que deben analizarse son:

- Política de seguridad.
- Organización de la seguridad de la información.
- Gestión de activos.
- Seguridad en los recursos humanos.
- Seguridad física y ambiental.
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de Sistemas de Información.
- Gestión de incidentes.
- Gestión de continuidad de negocio.
- Cumplimiento.

Esta apreciación de los 114 controles planteados por la norma para cumplir con los diferentes objetivos de control. Esta estimación la realizaremos según la siguiente tabla, que se basa en el Modelo de Madurez de la Capacidad (CMM):

| CONTROL | | | INICIAL | FINAL | EFECTIVIDAD | CMM |
|---|---|---|---|---|---|---|
| A.5 Information security policies | | | | | | |
| A.5.1 Management direction for information security | | | | | | |
| | A.5.1.1 | Policies for information security | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.5.1.2 | Review of the policies for information security | 1 - Inicial | 3 - Definido | 90% | L3 |
| A.6 Organization of information security | | | | | | |
| A.6.1 Internal organization | | | | | | |
| | A.6.1.1 | Information security roles and responsibilities | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.6.1.2 | Segregation of duties | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.6.1.3 | Contact with authorities | 0 - No existente | 2 - Repetible | 50% | L2 |
| | A.6.1.4 | Contact with special interest groups | 0 - No existente | 3 - Definido | 90% | L3 |
| | A.6.1.5 | Information security in project management | 0 - No existente | 3 - Definido | 90% | L3 |
| A.6.2 Mobile devices and teleworking | | | | | | |
| | A.6.2.1 | Mobile device policy | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.6.2.2 | Teleworking | 1 - Inicial | 3 - Definido | 90% | L3 |
| A.7 Human resource security | | | | | | |
| A.7.1 Prior to employment | | | | | | |
| | A.7.1.1 | Screening | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.7.1.2 | Terms and conditions of employment | 0 - No existente | 3 - Definido | 90% | L3 |
| A.7.2 During employment | | | | | | |
| | A.7.2.1 | Management responsibilities | 1 - Inicial | 4 - Gestionado | 95% | L4 |
| | A.7.2.2 | Information security awareness, education and training | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.7.2.3 | Disciplinary process | 1 - Inicial | 2 - Repetible | 50% | L2 |
| A.7.3 Termination and change of employment | | | | | | |
| | A.7.3.1 | Termination or change of employment responsibilities | 0 - No existente | 3 - Definido | 90% | L3 |
| A.8 Asset management | | | | | | |
| A.8.1 Responsibility for asset | | | | | | |
| | A.8.1.1 | Inventory of assets | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.8.1.2 | Ownership of assets | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.8.1.3 | Acceptable use of assets | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.8.1.4 | Return of assets | 1 - Inicial | 3 - Definido | 90% | L3 |
| A.8.2 Information classification | | | | | | |
| | A.8.2.1 | Classification of information | 2 - Repetible | 3 - Definido | 90% | L3 |
| | A.8.2.2 | Labelling of informa tion | 2 - Repetible | 3 - Definido | 90% | L3 |
| | A.8.2.3 | Handling of assets | 1 - Inicial | 3 - Definido | 90% | L3 |
| A.8.3 Media handling | | | | | | |
| | A.8.3.1 | Management of removable media | 1 - Inicial | 2 - Repetible | 50% | L2 |
| | A.8.3.2 | Disposal of media | 1 - Inicial | 2 - Repetible | 50% | L2 |
| | A.8.3.3 | Physical media transfer | 0 - No existente | 2 - Repetible | 50% | L2 |
| A.9 Access control | | | | | | |
| A.9.1 Business requirements of access control | | | | | | |
| | A.9.1.1 | Access control policy | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.9.1.2 | Access to networks and network services | 3 - Definido | 4 - Gestionado | 95% | L4 |
| A.9.2 User access management | | | | | | |
| | A.9.2.1 | User registration and de-registration | 1 - Inicial | 3 - Definido | 90% | L3 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | A.9.2.2 | User access provisioning | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.9.2.3 | Management of privileged access rights | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.9.2.4 | Management of secret authentication information of users | 0 - No existente | 2 - Repetible | 50% | L2 |
| | A.9.2.5 | Review of user access rights | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.9.2.6 | Removal or adjustment of access rights | 1 - Inicial | 3 - Definido | 90% | L3 |
| A.9.3 User responsibilities | | | | | | |
| | A.9.3.1 | Use of secret authentication information | 0 - No existente | 2 - Repetible | 50% | L2 |
| A.9.4 System and application access control | | | | | | |
| | A.9.4.1 | Information access restriction | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.9.4.2 | Secure log-on procedures | 2 - Repetible | 2 - Repetible | 50% | L2 |
| | A.9.4.3 | Password managment system | 0 - No existente | 3 - Definido | 90% | L3 |
| | A.9.4.4 | Use of privileged utility programs | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| | A.9.4.5 | Access control to program source code | 0 - No existente | 3 - Definido | 90% | L3 |
| A.10 Cryptography | | | | | | |
| A.10.1 Cryptographic controls | | | | | | |
| | A.10.1.1 | Policy on the use of cryptographic controls | 0 - No existente | 2 - Repetible | 50% | L2 |
| | A.10.1.2 | Key management | 0 - No existente | 2 - Repetible | 50% | L2 |
| A.11 Physical and environmental security | | | | | | |
| A.11.1 Secure areas | | | | | | |
| | A.11.1.1 | Physical security perimeter | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.11.1.2 | Physical entry controls | 2 - Repetible | 3 - Definido | 90% | L3 |
| | A.11.1.3 | Securing offices, rooms and facilities | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.11.1.4 | Protecting against external and environmental threats | 0 - No existente | 2 - Repetible | 50% | L2 |
| | A.11.1.5 | Working in secure areas | 0 - No existente | 3 - Definido | 90% | L3 |
| | A.11.1.6 | Delivery and loading areas | 1 - Inicial | 3 - Definido | 90% | L3 |
| A.11.2 Equipment | | | | | | |
| | A.11.2.1 | Equipment siting and protection | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| | A.11.2.2 | Supporting utilities | 2 - Repetible | 3 - Definido | 90% | L3 |
| | A.11.2.3 | Cabling security | 2 - Repetible | 3 - Definido | 90% | L3 |
| | A.11.2.4 | Equipment maintenance | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| | A.11.2.5 | Removal of assets | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.11.2.6 | Security of equipment and assets off-premises | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.11.2.7 | Secure disposal or reuse of equipment | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.11.2.8 | Unattended user equipment | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.11.2.9 | Clear desk and clear screen policy | 0 - No existente | 2 - Repetible | 50% | L2 |
| A.12 Operations security | | | | | | |
| A.12.1 Operational procedures and responsibilities | | | | | | |
| | A.12.1.1 | Documented operating procedures | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| | A.12.1.2 | Change management | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| | A.12.1.3 | Capacity management | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| | A.12.1.4 | Separation of development, testing and operational environments | 1 - Inicial | 3 - Definido | 90% | L3 |
| A.12.2 Protection from malware | | | | | | |
| | A.12.2.1 | Controls against malware | 0 - No existente | 3 - Definido | 90% | L3 |
| A.12.3 Backup | | | | | | |
| | A.12.3.1 | Information backup | 2 - Repetible | 3 - Definido | 90% | L3 |

| | | | | | | |
|---|---|---|---|---|---|---|
| A.12.4 Logging and monitoring | | | | | | |
| | A.12.4.1 | Event logging | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.12.4.2 | Protection of log information | 0 - No existente | 2 - Repetible | 50% | L2 |
| | A.12.4.3 | Administrator and operator logs | 0 - No existente | 2 - Repetible | 50% | L2 |
| | A.12.4.4 | Clock synchronisation | 0 - No existente | 3 - Definido | 90% | L3 |
| A.12.5 Control of operational software | | | | | | |
| | A.12.5.1 | Installation of software on operational systems | 1 - Inicial | 3 - Definido | 90% | L3 |
| A.12.6 Technical vulnerability management | | | | | | |
| | A.12.6.1 | Management of technical vulnerabilities | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.12.6.2 | Restrictions on software installation | 1 - Inicial | 3 - Definido | 90% | L3 |
| A.12.7 Information systems audit considerations | | | | | | |
| | A.12.7.1 | Information systems audit controls | 1 - Inicial | 3 - Definido | 90% | L3 |
| A.13 Communications security | | | | | | |
| A.13.1 Network security management | | | | | | |
| | A.13.1.1 | Network controls | 2 - Repetible | 3 - Definido | 90% | L3 |
| | A.13.1.2 | Security of network services | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| | A.13.1.3 | Segregation in networks | 0 - No existente | 4 - Gestionado | 95% | L4 |
| A.13.2 Information transfe | | | | | | |
| | A.13.2.1 | Information transfer policies and procedures | 0 - No existente | 2 - Repetible | 50% | L2 |
| | A.13.2.2 | Agreements on information transfer | 0 - No existente | 2 - Repetible | 50% | L2 |
| | A.13.2.3 | Electronic messaging | 0 - No existente | 2 - Repetible | 50% | L2 |
| | A.13.2.4 | Confidentiality or nondisclosure agreements | 4 - Gestionado | 5 - Optimizado | 100% | L5 |
| A.14 System acquisition, development and maintenance | | | | | | |
| A.14.1 Security requirements of information systems | | | | | | |
| | A.14.1.1 | Information security requirements analysis and specification | 2 - Repetible | 3 - Definido | 90% | L3 |
| | A.14.1.2 | Securing application services on public networks | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| | A.14.1.3 | Protecting application services transactions | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| A.14.2 Security in development and support processes | | | | | | |
| | A.14.2.1 | Secure development policy | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.14.2.2 | System change control procedures. | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.14.2.3 | Technical review of applications after operating platform | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.14.2.4 | Restrictions on changes to software packages | 0 - No existente | 2 - Repetible | 50% | L2 |
| | A.14.2.5 | Secure system engi neering principles | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.14.2.6 | Secure development environment | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.14.2.7 | Outsourced development | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.14.2.8 | System security testing | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| | A.14.2.9 | System acceptance testing | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| A.14.3 Test data | | | | | | |
| | A.14.3.1 | Protection of test data | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| A.15 Supplier relationships | | | | | | |
| A.15.1 Information security in supplier relationships | | | | | | |
| | A.15.1.1 | Information security policy for supplier relationships | 0 - No existente | 2 - Repetible | 50% | L2 |
| | A.15.1.2 | Addressing security within supplier agreements | 0 - No existente | 2 - Repetible | 50% | L2 |
| | A.15.1.3 | Information and communication technology supply chain | 0 - No existente | 2 - Repetible | 50% | L2 |

| | | | | | | |
|---|---|---|---|---|---|---|
| A.15.2 Supplier service delivery management | | | | | | |
| | A.15.2.1 | Monitoring and review of supplier services | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.15.2.2 | Managing changes to supplier services | 1 - Inicial | 2 - Repetible | 50% | L2 |
| A.16 Information security incident management | | | | | | |
| A.16.1 Management of information security incidents and improvements | | | | | | |
| | A.16.1.1 | Responsibilities and procedures | 3 - Definido | 5 - Optimizado | 100% | L5 |
| | A.16.1.2 | Reporting information security events | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| | A.16.1.3 | Reporting information security weaknesses | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.16.1.4 | Assessment of and decision on information security events | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| | A.16.1.5 | Response to information security incidents | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| | A.16.1.6 | Learning from information security incidents | 0 - No existente | 3 - Definido | 90% | L3 |
| | A.16.1.7 | Collection of evidence | 0 - No existente | 2 - Repetible | 50% | L2 |
| A.17 Information security aspects of business continuity management | | | | | | |
| A.17.1 Information security continuity | | | | | | |
| | A.17.1.1 | Planning information security continuity | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| | A.17.1.2 | Implementing information security continuity | 2 - Repetible | 4 - Gestionado | 95% | L4 |
| | A.17.1.3 | Verify, review and evaluate information security continuity | 1 - Inicial | 4 - Gestionado | 95% | L4 |
| A.17.2 Redundancies | | | | | | |
| | A.17.2.1 | Availability of information processing facilities | 1 - Inicial | 3 - Definido | 90% | L3 |
| A.18 Compliance | | | | | | |
| A.18.1 Compliance with legal and contractual requirements | | | | | | |
| | A.18.1.1 | Identification of applicable legislation and contractual requirements | 0 - No existente | 2 - Repetible | 50% | L2 |
| | A.18.1.2 | Illectual property rights | 0 - No existente | 2 - Repetible | 50% | L2 |
| | A.18.1.3 | Protection of records | 0 - No existente | 3 - Definido | 90% | L3 |
| | A.18.1.4 | Privacy and protection of personally identifiable information | 0 - No existente | 3 - Definido | 90% | L3 |
| | A.18.1.5 | Regulation of cryptographic controls | 0 - No existente | 2 - Repetible | 50% | L2 |
| A.18.2 Information security reviews | | | | | | |
| | A.18.2.1 | Independent review of information security | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.18.2.2 | Compliance with security policies and standards | 1 - Inicial | 3 - Definido | 90% | L3 |
| | A.18.2.3 | Technical compliance review | 0 - No existente | 3 - Definido | 90% | L3 |

*Tabla 21- CMM Controles ISO27001*

## 5.4 Presentación De Resultados.

Plasmar las valoraciones expuestas en el punto anterior nos ayuda tener una mejor comprensión de el estado actual una vez aplicados los proyectos.

Los controles y el nivel de madurez juegan un importante papel para la comprensión de la auditoria de cumplimiento, en el siguiente cuadro comparativo podemos ver como los controles han mejorado de manera notable después de la aplicación de los controles anexos a la norma.

Las siguientes tablas e ilustraciones proveen una visión más comprensible del estado de los controles antes y despues de la implementación del plan director.

| SITUACIÓN INICIAL | | |
|---|---|---|
| NIVEL (L) | CANT. CONTROLES | % |
| No existente | 35 | 30,70 |
| Inicial | 50 | 43,86 |
| Repetible | 26 | 22,81 |
| Definido | 2 | 1,75 |
| Gestionado | 1 | 0,88 |
| Optimizado | 0 | 0,00 |

*Tabla 22 - Controles CMM inicial*

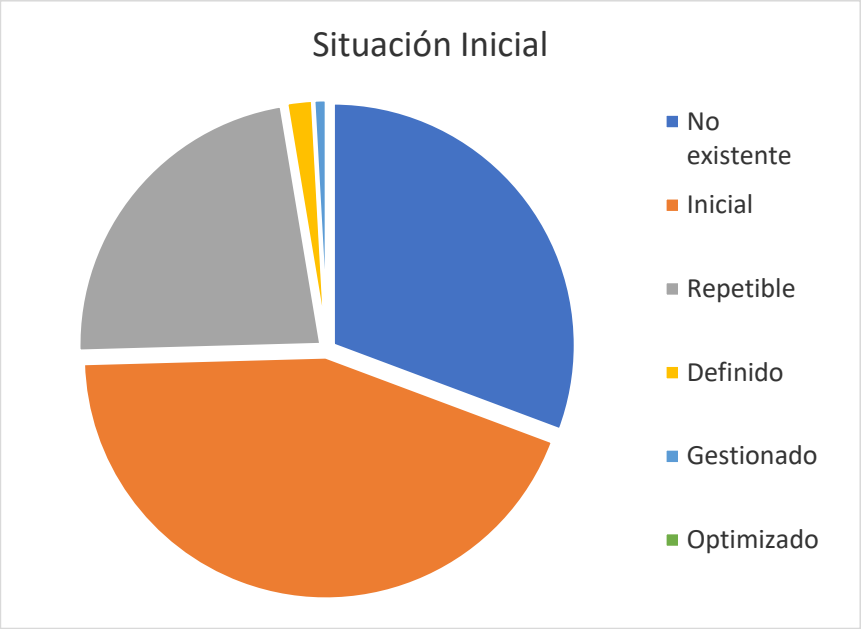



*Ilustración 5 - Controles CMM inicial.*

| SITUACIÓN FINAL | | |
|---|---|---|
| NIVEL (L) | CANT. CONTROLES | % |
| No existente | 0 | 0,00 |
| Inicial | 0 | 0,00 |
| Repetible | 26 | 22,81 |
| Definido | 65 | 57,02 |
| Gestionado | 21 | 18,42 |
| Optimizado | 2 | 1,75 |

*Tabla 23 - Controles CMM final*

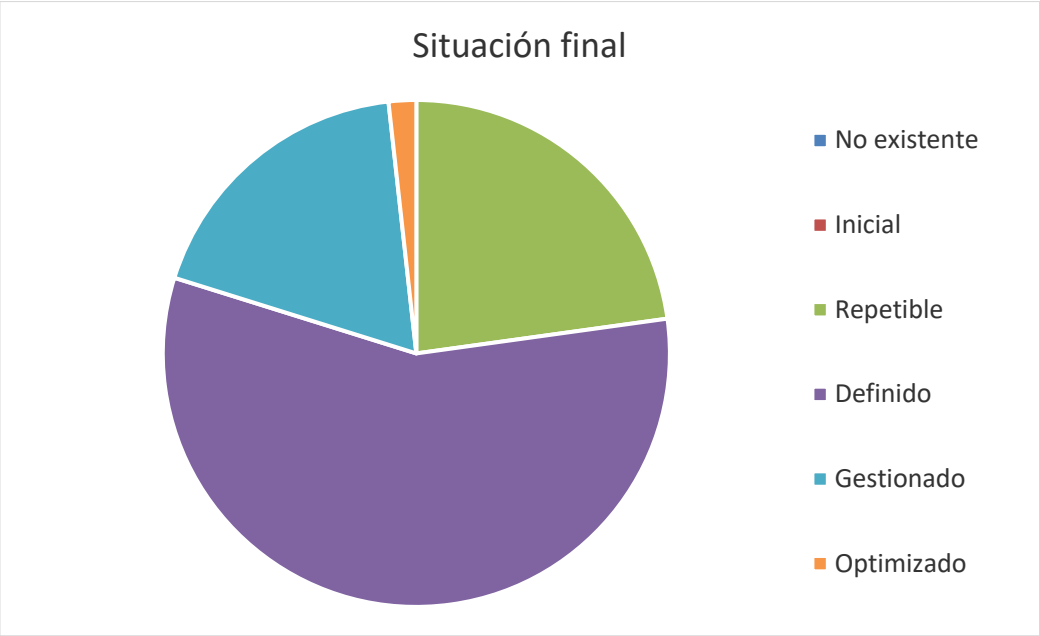



*Ilustración 6 - Controles CMM final*

Como referencia para nuestro análisis de no conformidades establecemos los siguientes criterios previo al despliegue de la auditoría propiamente dicha.

| TIPO | DESCRIPCIÓN |
|---|---|
| No conformidad mayor | Se incumple por completo un apartado del estándar |
| No conformidad menor | Se incumple un punto del estándar o se incumple un procedimiento propio de la organización. |
| Observación | No se incumple nada, pero si no se hace un tratamiento adecuado, en el futuro se puede convertir en no conformidad menor |
| Oportunidad de mejora | Es solo una recomendación, que nunca se convertirá ni en observación ni en no conformidad. |

*Tabla 24 - CMM no conformidades*

Siguiendo el procedimiento de auditorías detallado en el punto 2.2.2 del presente documento establecemos las no conformidades encontradas antes de los puntos de mejora. Las No Conformidades detectadas en el transcurso de la auditoria, se comentan y se analizan con el personal responsable del control auditado. Cada causa que produce la No Conformidad, y los efectos que conlleva la presencia de esta.
Las No Conformidades detectadas deben estar documentadas de forma precisa y concisa y basarse en datos objetivos.

| Controles | NO CONFORMIDADES | | | |
|---|---|---|---|---|
| | No conf. Mayor | No conf. Menor | Obsv. | Mejora |
| A.7 Human resource security | | | | |
| A.7.2 During employment | | | | |
| A.7.2.2 Information security awareness, education and training | X | | | |
| A.7.2.3 Disciplinary process | X | | | |
| A.9 Access control | | | | |
| A.9.2 User access management | | | | |
| A.9.2.4 Management of secret authentication information of users | | X | | |
| A.9.3 User responsibilities | | | | |
| A.9.3.1 Use of secret authentication information | | X | | |
| A.9.4 System and application access control | | | | |
| A.9.4.1 Information access restriction | | X | | |
| A.11 Physical and environmental security | | | | |
| A.11.1 Secure areas | | | | |
| A.11.1.2 Physical entry controls | | X | | |
| A.11.1.4 Protecting against external and environmental threats | | X | | |
| **A.18 Compliance.** | | | | |
| **A.18.1 Compliance with legal and contractual requirements.** | | | | |
| A.18.1.1 Identification of applicable legislation and contractual requirements | X | | | |

*Tabla 25 - No conformidades Controles.*

**FORMATO PDSI-FOR-002**

| FECHA | | |
|---|---|---|
| DIA | MES | AÑO |
| 30 | abril | 2021 |

**Resumen Ejecutivo No conformidades:**

| | |
|---|---|
| **No. No Conformidad:** | 1 |
| **Área:** | Seguridad ligada a RR.HH.. |
| **Tipo de No Conformidad:** | MAYOR |
| **Control incumplido:** | A.7.2.2 Concienciación , educación y capacitación en SI |
| **Descripción:** | No se realiza el procedimiento de inducción ni capacitación para el personal en temas de seguridad de la información. El manejo de responsabilidades en cuanto a los roles del personal no es perceptible. |
| **Acción Correctiva:** | Realizar seguimiento acerca de los planes de capacitación y procedimientos establecidos en cuanto a roles y responsabilidades. |
| **Fecha de Revisión:** | 20-abr-21 |

| | |
|---|---|
| **No. No Conformidad:** | 2 |
| **Área:** | Seguridad ligada a RR.HH.. |
| **Tipo de No Conformidad:** | MAYOR |
| **Control incumplido:** | A.7.2.3 Proceso disciplinario. |
| **Descripción:** | No existe procedimiento disciplinario para el desacato a las políticas de seguridad, ni para sancionar acciones que deriven en brechas de seguridad. |
| **Acción Correctiva:** | Realizar seguimiento acerca de los procedimientos establecidos en cuanto a sanciones administrativas. |
| **Fecha de Revisión:** | 27-abr-21 |

| | |
|---|---|
| **No. No Conformidad:** | 3 |
| **Área:** | Control de Acceso. |
| **Tipo de No Conformidad:** | MENOR |
| **Control incumplido:** | A 9.2.4 Gestión de la información secreta autenticación de usuario |
| **Descripción:** | Los sistemas de información y Las estaciones de trabajo cuentan con un sistema de autenticación pero las claves genéricas conocidas por el personal en su mayoría imposibilitan la confidencialidad de aquello. |

| | |
|---|---|
| **Acción Correctiva:** | Desplegar y hacer cumplir a cabalidad la política de seguridad de información, apartado usuarios y contraseñas, fijar obligatoriedad de cumplimiento al personal. |
| **Fecha de Revisión:** | 04-may-21 |

| | |
|---|---|
| **No. No Conformidad:** | 4 |
| **Área:** | Control de Acceso. |
| **Tipo de No Conformidad:** | MENOR |
| **Control incumplido:** | A 9.2.4 Gestión de la información secreta autenticación de usuario |
| **Descripción:** | Los sistemas de información y Las estaciones de trabajo cuentan con un sistema de autenticación pero las claves genéricas conocidas por el personal en su mayoría imposibilitan la confidencialidad de aquello. |
| **Acción Correctiva:** | Desplegar y hacer cumplir a cabalidad la política de seguridad de información, apartado usuarios y contraseñas, fijar obligatoriedad de cumplimiento al personal. |
| **Fecha de Revisión:** | 04-may-21 |

| | |
|---|---|
| **No. No Conformidad:** | 5 |
| **Área:** | Control de Acceso. |
| **Tipo de No Conformidad:** | MENOR |
| **Control incumplido:** | A 9.4.1 Restricción de acceso a información. |
| **Descripción:** | Los accesos a información sensible no se encuentran correctamente mapeados, y los privilegios de acceso a aplicaciones son muy generales. |
| **Acción Correctiva:** | Establecer perfiles de acceso y privilegios según las atribuciones y necesidades de usuarios. |
| **Fecha de Revisión:** | 04-may-21 |

| | |
|---|---|
| **No. No Conformidad:** | 6 |
| **Área:** | Control de Acceso. |
| **Tipo de No Conformidad:** | MENOR |

| | |
|---|---|
| **Control incumplido:** | A 11.1.2 Controles físicos de entrada. |
| **Descripción:** | Las áreas donde se almacena y se procesa información no cumplen con mecanismos de doble factor ni registro de entradas de personal. |
| **Acción Correctiva:** | Normar políticas de acceso de doble factor e implementar bitácora de ingresos y actividades. |
| **Fecha de Revisión:** | 11-may-21 |

| | |
|---|---|
| **No. No Conformidad:** | 7 |
| **Área:** | Control de Acceso. |
| **Tipo de No Conformidad:** | MENOR |
| **Control incumplido:** | A 11.1.4 Protección contra amenazas externas y ambientales. |
| **Descripción:** | Las instalaciones cuentan con protección básica solo contra incendios, no contra vandalismo ni a otras amenazas externas. |
| **Acción Correctiva:** | Normar una política de protección contra amenazas externas y levantar necesidades para adquirir protección contra estas. |
| **Fecha de Revisión:** | 18-may-21 |

| | |
|---|---|
| **No. No Conformidad:** | 8 |
| **Área:** | Cumplimiento |
| **Tipo de No Conformidad:** | MAYOR |
| **Control incumplido:** | A18.1.1 Identificación de legislación aplicable y requisitos contractuales. |
| **Descripción:** | La organización no observa requisitos legales ni regulatorios respecto a normas de control ni estándares de seguridad de información. |
| **Acción Correctiva:** | Inventariar leyes y estándares aplicables al sector gubernamental para normar la seguridad de la información institucional |
| **Fecha de Revisión:** | 25-may-21 |

| OBJETIVO |
|---|
| Auditar controles que presentan no conformidades en el SGSI de la organización. |
| **ALCANCE** |
| EL proceso se limita a revisión de controles la ISO/IEC:2013 , del SGSI de la EP Aguas de Manta. |
| **EQUIPO DE TRABAJO** |
| Auditor Líder.<br>Auditores.<br>Personal Técnico. |

| PROCESO | SUBPROCESO | PUNTOS DE NORMA |
|---|---|---|
| SGSI | Plan director. | ISO/IEC 27001:2013 |
| **PERSONA ( Responsable del Área)** | | |
| Ing. Antonio Segovia. | | |
| **DOCUMENTOS EXAMINADOS** | | |
| Plan director de SGSI<br>ISO/IEC:2013<br>FOR-PDSI-001 | | |

| DETALLES ADICIONALES | | | |
|---|---|---|---|
| La auditoría del SGSI implantado refleja varias no conformidades respecto a los controles anexos a la norma, los cuales fueron auditados de manera métodica según la programación anexa. | | | |
| **No.** | **DESCRIPCIÓN** | **DEBILIDADES** | **OPORTUNIDADES** |
| **1** | El proceso de auditoria contó con apoyo directivo. | Hubo resistencia del personal. | Directrices de autoridades. |
| **2** | La auditoría se llevo a cabo según el cronograma. | Desfase en fechas. | Mejora de tiempos en varios controles. |
| **3** | Seguimiento y evaluación. | No consecución. | Mejora continua esquematizada. |
| **OBSERVACIONES** | | | |
| Los resultados de las pruebas objetivas fueron analizados en un marco de trabajo previamente definido en el alcance, bajo la métodología establecida, haciendo match con la pólitica de seguridad de información de EP Aguas de Manta . Los hallazgos que contengan consideraciones de seguridad críticas, y las no conformidades mayores deben ser tratados con el cómite de seguridad de información. | | | |

## 6. Presentación de resultados y entrega de informes.

Presentación ejecutiva de powerpoint, insumo final del trabajo.

# 7. Anexos

*Anexo 1 – PDSI-FOR-001*

AGUAS de MANTA

## PROGRAMA DE AUDITORÍA SGSI

### 1- OBJETIVO Y ALCANCE DE AUDITORIA

| |
|---|
| **OBJETIVO DEL PROGRAMA: Auditoria del SGSI**<br><br>**ALCANCE: Revisión plurianual de los controles del anexo A ISO/IEC 27001 :2013** |

### RESPONSABILIDADES

| | |
|---|---|
| **AUDITOR LÍDER:** | |
| **ESPECIALISTA TECNICO:** | |
| **AUDITOR INTERNO:** | |

### 2- CALENDARIO Y SEGUIMIENTO DEL PROGRAMA

| | | | AÑO | | |
|---|---|---|---|---|---|
| **CONTROL** | | | **2021** | **2022** | **2023** |
| A.5 Information security policies | | | | | |
| | A.5.1 Management direction for information security | | | | |
| | | A.5.1.1 Policies for information security | X | | |
| | | A.5.1.2 Review of the policies for information security | X | | |
| A.6 Organization of information security | | | X | | |
| | A.6.1 Internal organization | | | | |
| | | A.6.1.1 Information security roles and responsibilities | X | | |
| | | A.6.1.2 Segregation of duties | X | | |
| | | A.6.1.3 Contact with authorities | X | | |
| | | A.6.1.4 Contact with special interest groups | X | | |
| | | A.6.1.5 Information security in project management | X | | |
| | A.6.2 Mobile devices and teleworking | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | A.6.2.1 | Mobile device policy | | X | |
| | | A.6.2.2 | Teleworking | | X | |
| A.7 Human resource security | | | | | | |
| | A.7.1 Prior to employment | | | | | |
| | | A.7.1.1 | Screening | X | | |
| | | A.7.1.2 | Terms and conditions of employment | X | | |
| | A.7.2 During employment | | | | | |
| | | A.7.2.1 | Management responsibilities | | X | |
| | | A.7.2.2 | Information security awareness, education and training | | X | |
| | | A.7.2.3 | Disciplinary process | | X | |
| | A.7.3 Termination and change of employment | | | | | |
| | | A.7.3.1 | Termination or change of employment responsibilities | | X | |
| A.8 Asset management | | | | | | |
| | A.8.1 Responsibility for asset | | | | | |
| | | A.8.1.1 | Inventory of assets | | X | |
| | | A.8.1.2 | Ownership of assets | | X | |
| | | A.8.1.3 | Acceptable use of assets | | X | |
| | | A.8.1.4 | Return of assets | | X | |
| | A.8.2 Information classification | | | | | |
| | | A.8.2.1 | Classification of information | X | | |
| | | A.8.2.2 | Labelling of informa tion | X | | |
| | | A.8.2.3 | Handling of assets | X | | |
| | A.8.3 Media handling | | | | | |
| | | A.8.3.1 | Management of removable media | | | X |
| | | A.8.3.2 | Disposal of media | | | X |
| | | A.8.3.3 | Physical media transfer | | | X |
| A.9 Access control | | | | | | |
| | A.9.1 Business requirements of access control | | | | | |
| | | A.9.1.1 | Access control policy | | X | |
| | | A.9.1.2 | Access to networks and network services | | X | |
| | A.9.2 User access management | | | | | |
| | | A.9.2.1 | User registration and de-registration | | X | |
| | | A.9.2.2 | User access provisioning | | X | |
| | | A.9.2.3 | Management of privileged access rights | | X | |
| | | A.9.2.4 | Management of secret authentication information of users | | X | |
| | | A.9.2.5 | Review of user access rights | | X | |
| | | A.9.2.6 | Removal or adjustment of access rights | | X | |
| | A.9.3 User responsibilities | | | | | |
| | | A.9.3.1 | Use of secret authentication information | | | X |
| | A.9.4 System and application access control | | | | | |
| | | A.9.4.1 | Information access restriction | | | X |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | A.9.4.2 | Secure log-on procedures | | | X |
| | | A.9.4.3 | Password managment system | | | X |
| | | A.9.4.4 | Use of privileged utility programs | | | X |
| | | A.9.4.5 | Access control to program source code | | | X |
| A.10 Cryptography | | | | | | |
| | A.10.1 Cryptographic controls | | | | | |
| | | A.10.1.1 | Policy on the use of cryptographic controls | | | X |
| | | A.10.1.2 | Key management | | | X |
| A.11 Physical and environmental security | | | | | | |
| | A.11.1 Secure areas | | | | | |
| | | A.11.1.1 | Physical security perimeter | X | | |
| | | A.11.1.2 | Physical entry controls | X | | |
| | | A.11.1.3 | Securing offices, rooms and facilities | X | | |
| | | A.11.1.4 | Protecting against external and environmental threats | X | | |
| | | A.11.1.5 | Working in secure areas | X | | |
| | | A.11.1.6 | Delivery and loading areas | X | | |
| | A.11.2 Equipment | | | | | |
| | | A.11.2.1 | Equipment siting and protection | | X | |
| | | A.11.2.2 | Supporting utilities | | X | |
| | | A.11.2.3 | Cabling security | | X | |
| | | A.11.2.4 | Equipment maintenance | | X | |
| | | A.11.2.5 | Removal of assets | | X | |
| | | A.11.2.6 | Security of equipment and assets off-premises | | X | |
| | | A.11.2.7 | Secure disposal or reuse of equipment | | X | |
| | | A.11.2.8 | Unattended user equipment | | X | |
| | | A.11.2.9 | Clear desk and clear screen policy | | X | |
| A.12 Operations security | | | | | | |
| | A.12.1 Operational procedures and responsibilities | | | | | |
| | | A.12.1.1 | Documented operating procedures | | | X |
| | | A.12.1.2 | Change management | | | X |
| | | A.12.1.3 | Capacity management | | | X |
| | | A.12.1.4 | Separation of development, testing and operational environments | | | X |
| | A.12.2 Protection from malware | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | A.12.2.1 | Controls against malware | | X | |
| | A.12.3 Backup | | | | | |
| | | A.12.3.1 | Information backup | | X | |
| | A.12.4 Logging and monitoring | | | | | |
| | | A.12.4.1 | Event logging | X | | |
| | | A.12.4.2 | Protection of log information | X | | |
| | | A.12.4.3 | Administrator and operator logs | X | | |
| | | A.12.4.4 | Clock synchronisation | X | | |
| | A.12.5 Control of operational software | | | | | |
| | | A.12.5.1 | Installation of software on operational systems | | X | |
| | A.12.6 Technical vulnerability management | | | | | |
| | | A.12.6.1 | Management of technical vulnerabilities | X | | |
| | | A.12.6.2 | Restrictions on software installation | X | | |
| | A.12.7 Information systems audit considerations | | | | | |
| | | A.12.7.1 | Information systems audit controls | | | X |
| A.13 Communications security | | | | | | |
| | A.13.1 Network security management | | | | | |
| | | A.13.1.1 | Network controls | | X | |
| | | A.13.1.2 | Security of network services | | X | |
| | | A.13.1.3 | Segregation in networks | | X | |
| | A.13.2 Information transfe | | | | | |
| | | A.13.2.1 | Information transfer policies and procedures | | X | |
| | | A.13.2.2 | Agreements on information transfer | | X | |
| | | A.13.2.3 | Electronic messaging | | X | |
| | | A.13.2.4 | Confidentiality or nondisclosure agreements | | X | |
| A.14 System acquisition, development and maintenance | | | | | | |
| | A.14.1 Security requirements of information systems | | | | | |
| | | A.14.1.1 | Information security requirements analysis and specification | X | | |
| | | A.14.1.2 | Securing application services on public networks | X | | |
| | | A.14.1.3 | Protecting application services transactions | X | | |
| | A.14.2 Security in development and support processes | | | | | |
| | | A.14.2.1 | Secure development policy | | X | |
| | | A.14.2.2 | System change control procedures. | | X | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | A.14.2.3 | Technical review of applications after operating platform | | X | |
| | | A.14.2.4 | Restrictions on changes to software packages | | X | |
| | | A.14.2.5 | Secure system engine neering principles | | X | |
| | | A.14.2.6 | Secure development environment | | X | |
| | | A.14.2.7 | Outsourced development | | X | |
| | | A.14.2.8 | System security testing | | X | |
| | | A.14.2.9 | System acceptance testing | | X | |
| | A.14.3 Test data | | | | | |
| | | A.14.3.1 | Protection of test data | | X | |
| A.15 Supplier relationships | | | | | | |
| | A.15.1 Information security in supplier relationships | | | | | |
| | | A.15.1.1 | Information security policy for supplier relationships | | | X |
| | | A.15.1.2 | Addressing security within supplier agreements | | | X |
| | | A.15.1.3 | Information and communication technology supply chain | | | X |
| | A.15.2 Supplier service delivery management | | | | | |
| | | A.15.2.1 | Monitoring and review of supplier services | | | X |
| | | A.15.2.2 | Managing changes to supplier services | | | X |
| A.16 Information security incident management | | | | | | |
| | A.16.1 Management of information security incidents and improvements | | | | | |
| | | A.16.1.1 | Responsibilities and procedures | X | | |
| | | A.16.1.2 | Reporting information security events | X | | |
| | | A.16.1.3 | Reporting information security weaknesses | X | | |
| | | A.16.1.4 | Assessment of and decision on information security events | X | | |
| | | A.16.1.5 | Response to information security incidents | X | | |
| | | A.16.1.6 | Learning from information security incidents | X | | |
| | | A.16.1.7 | Collection of evidence | X | | |
| A.17 Information security aspects of business continuity management | | | | | | |
| | A.17.1 Information security continuity | | | | | |
| | | A.17.1.1 | Planning information security continuity | | X | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | A.17.1.2 | Implementing information security continuity | | X | |
| | | A.17.1.3 | Verify, review and evaluate information security continuity | | X | |
| | A.17.2 Redundancies | | | | | |
| | | A.17.2.1 | Availability of information processing facilities | | | |
| A.18 Compliance | | | | | | X |
| | A.18.1 Compliance with legal and contractual requirements | | | | | |
| | | A.18.1.1 | Identification of applicable legislation and contractual requirements | | | X |
| | | A.18.1.2 | Illectual property rights | | | X |
| | | A.18.1.3 | Protection of records | | | X |
| | | A.18.1.4 | Privacy and protection of personally identifiable information | | | X |
| | | A.18.1.5 | Regulation of cryptographic controls | | | X |
| | A.18.2 Information security reviews | | | | | |
| | | A.18.2.1 | Independent review of information security | | | X |
| | | A.18.2.2 | Compliance with security policies and standards | | | X |
| | | A.18.2.3 | Technical compliance review | | | X |

**RECURSOS DEL PROGRAMA:**

| **ELEMENTO FINANCIERO** | | | | **($)** |
|---|---|---|---|---|
| PRESUPUESTO REFRENCIAL | | | | |
| INSUMOS | | | | |
| SERVICIOS PROFESIONALES | | | | |
| **OBSERVACIONES** | | | | |
| | | | | |

*Anexo 1 – PDSI-FOR-002*

**No:**

| FECHA | | |
|---|---|---|
| **DIA** | **MES** | **AÑO** |
| | | |

**Resumen Ejecutivo:**

| **OBJETIVO** |
|---|
| |
| **ALCANCE** |
| |
| **EQUIPO DE TRABAJO** |
| |

| **PROCESO** | **SUBPROCESO** | **PUNTOS DE NORMA** |
|---|---|---|
| | | |
| **PERSONA ( Responsable del Área)** | | |
| | | |
| **DOCUMENTOS EXAMINADOS** | | |
| | | |

| **DETALLES ADICIONALES** | | | |
|---|---|---|---|
| | | | |
| **No.** | **DESCRIPCION** | **DEBILIDADES** | **OPORTUNIDADES** |
| | | | |
| | | | |
| **OBSERVACIONES** | | | |
| | | | |

# 8. Glosario.

**Auditor Líder:** Persona designada por el Representante de la Gerencia en cada auditoría interna para coordinarla.

**Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría.

**Dirección:** Se refiere a las autoridades, miembros de la alta gerencia, directores, asesores y todos los cargos tomadores inmerso en la toma de decisiones.

**EGSI:** Esquema gubernamental de Seguridad de Información. (normativa ecuatoriana)

**Equipo Auditor:** Uno o más auditores que llevan a cabo una auditoria.

**Evidencia Objetiva**: Información cuya veracidad puede demostrarse, basada en hechos obtenidos por observación, medición, ensayo u otros medios.

**IEC:** International Electrotechnical Comission (Comisión Electrotécnica Internacional) .

**ISO:** International Standards Organization (Organización Internacional de Estándares).

**LOGS (registros):** Término para definir datos que detallan quién, qué, cuándo, dónde y porqué un evento ocurre para un sistema informático especificado.

**SGSI**: Sistema de gestión de seguridad de Información.

**Sistemas de información (SI) :** Software que se ha desarrollado o personalizado con el fin de automatizar procesos institucionales.

# 9. Bibliografía.


- https://advisera.com/27001academy/es/que-es-iso-27001/
- http://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/
- http://www.pmg-ssi.com/2015/05/iso-27001-analizar-y-gestionar-riesgos-sgsi/
- https://www.ccn-cert.
- CUERVO ALVAREZ, SARA , Implementación ISO 27001. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64827/8/scuervoTFM0617memoria.pdf
- MARIBEL AVILA ARZUZA , Implementación SGSI. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/14743/1/mavilaarzTFM0612memoria.pdf