**ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**


**Facultad de Ingeniería en Electricidad y Computación**

# “DESARROLLO DE UN ESQUEMA DE SEGURIDAD Y PLAN DE CONTINGENCIA PARA UN CENTRO DE INVESTIGACIÓN"

**TRABAJO DE TITULACIÓN**

PREVIA A LA OBTENCIÓN DEL TÍTULO DE:

**MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA**

Presentado por:

ANDREA SOLANGE FREIRE MORAN

PRISCILA ELIZABETH BERNAL ORTIZ

GUAYAQUIL – ECUADOR

2017

# AGRADECIMIENTO

A Dios por ser pilar fundamental en nuestra vida y estar presente en todos los pasos que damos.

A nuestros padres porque siempre nos han apoyado de manera incondicional y sin ellos no hubiese sido posible alcanzar esta meta.

A la Ing. Karina Astudillo por ser una excelente profesional al brindarnos todos sus conocimientos y ayudarnos en la realización de este trabajo.

# DEDICATORIA

A mi familia de manera especial a mis hijos por ser mi mayor bendición, motivación e impulso, así también a mis padres por ser mi mejor ejemplo a seguir y por brindarme todo su amor y apoyo incondicionales.

Priscila Bernal

Dedico este trabajo a mi familia que es el pilar de todos mis logros, a mi madre y a mis hermanas que siempre me apoyan en todo, a mi padre siempre me transmitió constancia y a pesar de nuestra distancia física siento que está conmigo siempre y aunque nos faltaron muchas cosas por vivir juntos, sé que este momento hubiera sido especial para él tanto como lo es para mí.

Andrea Freire

# TRIBUNAL DE SUSTENTACIÓN

_____

MSIG. LENIN FREIRE COBOS

DIRECTOR MSIA

_____

MSIG. LENIN FREIRE COBOS

DIRECTOR DEL PROYECTO DE GRADUACIÓN

_____

MSIG. NESTOR ARREAGA

MIEMBRO DEL TRIBUNAL

# DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

(Reglamento de exámenes y títulos profesionales de la ESPOL)

# RESUMEN

El presente trabajo de Titulación presenta el análisis, desarrollo e implementación de un Esquema de Seguridad informático para un Centro de Investigación climático, el mismo que ha sido desarrollado basado en las normas para el análisis de riesgo establecidas por el Instituto Nacional de Estándares y Tecnología (NIST), y los controles y políticas de seguridad según la Norma Internacional para seguridad de la información ISO 27001 emitida por la Organización Internacional de Normalización (ISO).

Debido a que la información actualmente es el activo más importante de toda Organización, está debe ser protegida contra cualquier tipo de amenaza que comprometa su confidencialidad, integridad y disponibilidad. Por ello creemos que la implementación de un esquema de seguridad informático que permita asegurar de manera eficaz y eficiente este activo tan importante, es de suma importancia para el Centro Internacional para la Investigación del Fenómeno del Niño (CIIFEN).

# ÍNDICE GENERAL

# ABREVIATURAS Y SIMBOLOGÍA

| | | |
|---|---|---|
| **CIIFEN** | **:** | Centro Internacional para la Investigación del Fenómeno del Niño |
| **ISO** | **:** | Organización Internacional de Normalización |
| **NIST** | **:** | Instituto Nacional de Estándares y Tecnología |
| **SGSI** | **:** | Sistema de Gestión de la Seguridad de la Información |
| **SQL** | **:** | Structured Query Language |
| **WEB** | **:** | World Wide Web |

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# INTRODUCCIÓN

La información actualmente se ha convertido en uno de los activos más valiosos de toda empresa, por lo cual se vuelve imprescindible asegurarla de manera eficiente en tres aspectos básicos que son su confidencialidad, disponibilidad e integridad, para esto es necesario conocer y aplicar distintas normas de seguridad de la información. Así como implementar esquemas de seguridad que garanticen la protección de la información contra daño o robo.

El Centro Internacional para la Investigación del Fenómeno del Niño (CIIFEN) se dedica a la investigación sobre el clima y la divulgación de información climática de diferente tipo cómo pronóstico estacional y vulnerabilidades ambientales y climáticas las cuáles son de gran importancia para sus clientes. Por este motivo, el CIIFEN requiere que

su información sea resguardada de cualquier tipo de amenaza contra su integridad, confidencialidad y disponibilidad, siendo justamente este el objetivo que se pretende con la realización del presente trabajo, el cual consiste en la implementación de un Esquema de Seguridad para el Centro de Investigación Climático.

El esquema de Seguridad planteado ha sido implementado siguiendo las diferentes normas técnicas de Seguridad descritas por Normas Internacionales de Seguridad de la Información, como son las Normas del Instituto Nacional de Estándares y Tecnología (NIST), y también por las Normas ISO 27001 de la Organización Internacional de Normalización (ISO). Las cuáles nos han brindado la metodología adecuada para desarrollar una serie de pasos para implementar controles y políticas de seguridad, que mitiguen las amenazas y vulnerabilidades del principal Sistema del Centro el cuál es el de Envío masivo de Boletines, para encontrar dichas amenazas y establecer cuáles son las más críticas se realizó el correspondiente análisis de riesgo, mediante la guía del conjunto de Normas para seguridad de la información establecidas por el NIST.

Finalmente se desarrolló un procedimiento de aseguramiento de un servidor previo su puesta en producción, el mismo que será de gran ayuda para el Centro de Investigación, puesto que no poseían ningún tipo de seguridad para este activo tan importante como lo es el Servidor del Sistema de envío masivo de boletines, y contar con esta seguridad, les garantiza que la información contenida en dicho activo también se encuentre protegida, al contar con un proceso integral para mitigar los riesgos a los que está expuesto un Servidor si no se instala con todas las medidas de seguridad requeridas para su óptima instalación y posterior puesta en producción.

# CAPÍTULO 1

## GENERALIDADES

### 1.1 Antecedentes

El Centro de investigación es un organismo internacional encargado de la investigación aplicada del clima aparte de estos brinda servicios climáticos para la región oeste de Sudamérica. Los servicios que brinda el centro de investigación son los siguientes:

• Envío de boletines quincenales sobre climatología y pronóstico estacional.

• Conferencias sobre clima, ambiente, vulnerabilidad ambiental y climática, adaptación al cambio climático.

• Desarrollo y ejecución de proyectos sobre vulnerabilidad ambiental y climática, clima y cambio climático.

• Creación de contenidos sobre vulnerabilidad ambiental y climática, clima y cambio climático.

• Transferencia de Tecnologías a los servicios meteorológicos de la región oeste de Sudamérica.

Desde sus inicios hace más de 10 años mantienen el área de tecnologías de información como un área de desarrollo de aplicativos relacionados con el área ambiental y climática paralelos a los proyectos que se desarrollan y almacenamiento de los mismos. En la medida que ha pasado el tiempo ha acumulado estos sistemas y se han adicionado más funciones ajenas al desarrollo de sistemas y soporte de equipos con lo cual ha crecido el área de tecnologías de información.

El crecimiento del área de tecnologías de información se ha dado a nivel técnico, pero no ha tenido repercusiones en cuanto a gestión tecnológica dentro del centro de investigación. Se ha tenido varias iniciativas para segregación de funciones y de creación de documentación de gestión del área de tecnologías de información, pero el área técnica de desarrollo de proyectos siempre ha sido una prioridad para el centro de investigación.

Actualmente, el centro se está enfocando en mejorar esto porque se han dado varios problemas técnicos e incidentes de seguridad originados por

falla de gestión tecnológica y también se han originado incidentes por no tener una planificación de las contingencias; por lo cual se ha visto en la necesidad de la creación de un esquema de seguridad informática y en la creación de un plan de contingencia para el área de tecnologías de la información.

## 1.2 Descripción del Problema

De lo observado en el transcurso del trabajo del centro, las operaciones que se realizan en el aspecto informático son las siguientes:

• Envió de boletines y contenido masivo por correo electrónico.

• Manejo de contenidos web.

• Acceso a internet por parte de los funcionarios.

• Desarrollo de Aplicativos por proyectos (Los que más tienden a estar más expuestos son las aplicaciones web)

• Redes wifi

• Red de Área Local

• Usuarios Locales

Existe información sensible del desarrollo de proyectos del centro que actualmente solo se encuentra en las máquinas de los funcionarios que

se encuentran involucrados en el proyecto, la información técnica se encuentra en un servidor Windows -así mismo como el servidor de aplicaciones contable- que es accesible desde la red inalámbrica, no existen las debidas configuraciones de red para el seccionamiento de la misma y esta es la misma red que se usa para las conferencias.

Existen inconvenientes en la red local está fallando el acceso al internet y no se han identificado las causas de este fallo, hay un fallo en la seguridad en uno de los servidores externos que se encuentran en la red local. Hay servidores con versiones de sistemas operativos antiguas lo cual los vuelve bastante vulnerable a los ataques cibernéticos.

El manejador de contenido que tiene actualmente en el centro funciona bajo una versión antigua lo cual ha generado inconvenientes en el pasado como borrado del sitio completo, otro incidente que sucedió es que dieron de baja en el hosting del sitio puesto que se encontraba dentro un sitio fraudulento de un banco de Norteamérica.

El centro actualmente no tiene un esquema de seguridad que siga alguna de las normas y estándares de la industria, si bien tiene lo básico en seguridad a nivel técnico, pero no tiene un esquema lógico y una documentación del mismo.

El centro actualmente no tiene en un nivel de prioridad alto el concepto de prevención en el área informática. La forma de resolver los incidentes

es de manera reactiva por lo que genera una pérdida de capital que se podría haber reducido invirtiendo en soluciones preventivas.

El centro actualmente no cuenta con una documentación de procesos para el área de tecnologías de la información funciona con los procedimientos tradicionales que se tiene en un área de sistemas; el área de tecnologías de la información ha crecido durante este último año puesto que antes las funciones de sistemas se limitaban a mantenimiento de equipos.

## 1.3 Solución Propuesta

Implementación de procedimientos para cada una de las actividades que realiza el área informática del centro. - Se realizará un listado de procesos ofrecidos por el área de tecnologías de la información hacia el centro. Se generará documentación de procedimientos a realizarse por el área de tecnologías de información.

Implementación de políticas de seguridad. - Se realizará un análisis de riesgo el cual determinará la implementación de políticas de seguridad de acuerdo al listado de procesos generados y el listado de activos.

Rediseño de la estructura de la red y seccionamiento de la red en diferentes subredes por áreas. - Se procederá al segmentar la red en subredes, con lo cual se configurará vlans, de ser posible reemplazar el

servidor intermediario entre la red local y la red pública por un router y configurar de manera perimetral un firewall.

Identificación del proceso principal del Centro y de sus activos, realización del análisis de riesgo mediante la identificación de las amenazas y vulnerabilidades y las correspondientes medidas de seguridad o controles para los activos más críticos, mediante la aplicación de las diferentes normas de seguridad de la información como las NIST 800-30 e ISO 27001.

## 1.4 Objetivo General

Desarrollar un esquema de seguridad que incluya procedimientos, políticas, controles de seguridad y soluciones de tecnologías de información para un centro de investigación, así como realizar un procedimiento de aseguramiento de servidores previo su puesta en producción.

## 1.5 Objetivo Específicos

Los objetivos específicos son los siguientes:

1. Diseño de un esquema de seguridad.
2. Realizar un análisis de riesgo del principal proceso del Centro y de sus activos.

3. Desarrollar políticas y controles de seguridad informática.

4. Implementar un procedimiento de aseguramiento de un servidor previo su puesta en producción para la disminución del daño en una contingencia.

## 1.6 Metodología

Para la creación del esquema de seguridad se seguirán la siguiente metodología:

• Definición de los procesos.

• Asociación de los activos de información al proceso critico.

• Definición de los criterios de seguridad de los activos.

• Realización de un análisis de vulnerabilidad y amenazas a los activos.

• Realización de un análisis de riesgos.

• Realización de un análisis de tratamiento de riesgos.

Se realizará la Evaluación de Riesgo del CIIFEN utilizando la metodología descrita en la publicación especial 800-30 del Instituto Nacional de Estándares y Tecnología (NIST) Guía de gestión de riesgos de sistemas de tecnologías de información, conjuntamente con la creación del Plan de Seguridad del Sistema, en el cual se evaluará los

recursos y controles necesarios para administrar y eliminar vulnerabilidades que pueden ser explotadas por amenazas internas o externas al Centro, las vulnerabilidades son debilidades que pueden ser explotadas por una amenaza o grupo de amenazas. Estas vulnerabilidades pueden ser mitigadas por Salvaguardias recomendadas. Las salvaguardias son características y controles de seguridad que, cuando se agregan o se incluyen en el entorno de tecnología de la información, mitigan el riesgo asociado con la operación, a niveles manejables. El alcance de la evaluación de riesgo se centrará en los controles aplicables al entorno del sistema en las áreas de software, hardware, redes de comunicación e información.

Esta evaluación de riesgos proporcionará una evaluación cualitativa estructurada del entorno operativo. Abordando la sensibilidad, las amenazas, las vulnerabilidades, los riesgos y las salvaguardias. Las Salvaguardias realizadas en esta evaluación de riesgo, deberán por tanto ser aplicadas por el CIIFEN ya que de no hacerlo el resultado podría ser la modificación o destrucción de datos, la divulgación de información sensible o la denegación de servicio a los usuarios que requieren la información con frecuencia.

# CAPÍTULO 2

## MARCO TEÓRICO

### 2.1 Normas y estándares necesarios para la implementación.

En [1] podemos encontrar la siguiente definición: “Las organizaciones necesitan demostrar que realizan una gestión competente y efectiva de la seguridad de los recursos y datos que gestionan.

− Deben demostrar que identifican y detectan los riesgos a los que está sometida y que adoptan medidas adecuadas y proporcionadas.

− Es necesario un conjunto estructurado, sistemático, coherente y completo de normas a seguir.”

De lo anterior podemos decir pues que toda organización necesita de alguna forma asegurar que están realizando un proceso eficiente

para resguardar de manera adecuada la información y los recursos que disponen. Una forma de lograr esto es siendo capaces de identificar las posibles vulnerabilidades a los que se encuentran expuestos y además de ello dar las soluciones efectivas para dichas vulnerabilidades es decir minimizar el riesgo con acciones correctivas oportunas, así también es indispensable que cuenten con una metodología bien definida de estándares y normas que se deben aplicar. Son justamente el conjunto de normas ISO 27000 las que nos dan las directrices a seguir.

## 2.2 SGSI

Una de las herramientas más importantes hoy en día dentro de la seguridad informática es sin duda el SGSI (Sistema de Gestión de la Seguridad de la Información) o de sus siglas en ingles ISMS (Information Security Management System), el cual nos brinda un proceso ordenado y con la documentación necesaria al alcance de todos los miembros de la organización para que se pueda asegurar la información de manera eficiente y efectiva.

En [2] podemos encontrar la siguiente definición: “Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos

relevantes adoptados para garantizar su C-I-D (Confidencialidad, Integridad, Disponibilidad):

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática,

estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías."

## 2.3 ISO 27001

En [3] podemos encontrar la siguiente definición: "ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001."

Según la norma ISO 27001 la seguridad de la información radica en la conservación de su confidencialidad, integridad y disponibilidad al

igual que la forma en que se gestionan sus sistemas dentro de la empresa.

**¿Qué es la ISO 27001?**

En [4], podemos encontrar la siguiente definición: “Sistemas de Gestión la Seguridad de la Información ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización. La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

**Estructura de la norma ISO 27001**

Objeto y campo de aplicación: La norma comienza aportando unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar.

Referencias Normativas: Recomienda la consulta de ciertos documentos indispensables para la aplicación de ISO 27001.

Términos y Definiciones: Describe la terminología aplicable a este estándar.

Contexto de la Organización: Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI.

Liderazgo: Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma.

Planificación: Esta es una sección que pone de manifiesto la importancia de la determinación de riesgos y oportunidades a la hora de planificar un Sistema de Gestión de Seguridad de la Información, así como de establecer objetivos de Seguridad de la Información y el modo de lograrlos.

Soporte: En esta cláusula la norma señala que para el buen funcionamiento del SGSI la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso.

Operación: Para cumplir con los requisitos de Seguridad de la Información, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la Seguridad de la Información y un tratamiento de ellos.

Evaluación del Desempeño: En este punto se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del Sistema de Gestión de Seguridad de la Información, para asegurar que funciona según lo planificado.

Mejora: Por último, se encuentran las obligaciones que tiene una organización cuando encuentra una no conformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del SGSI."

## 2.4 NIST 800-30

En [5] nos encontramos que las organizaciones de los sectores público y privado dependen de la tecnología de la información y de

los sistemas de información para llevar a cabo con éxito sus misiones y funciones empresariales. Los sistemas de información pueden incluir entidades muy diversas, desde redes de oficinas, sistemas financieros y de personal hasta sistemas muy especializados. Los sistemas de información están sujetos a serias amenazas que pueden tener efectos adversos sobre las operaciones y los activos de la organización, las personas, otras organizaciones y la Nación al explotar vulnerabilidades conocidas y desconocidas para comprometer la confidencialidad, integridad o disponibilidad de la información que se procesa, o transmite por dichos sistemas.

Las amenazas a los sistemas de información pueden incluir ataques intencionados, interrupciones ambientales, errores humanos / de máquina y fallas estructurales, y pueden resultar en perjuicio para los intereses de seguridad nacional y económico de los Estados Unidos. Por lo tanto, es imperativo que los líderes y gerentes de todos los niveles entiendan sus responsabilidades y sean responsables por la gestión del riesgo de seguridad de la información, es decir, el riesgo asociado con el funcionamiento y uso de sistemas de información que respalden las misiones y las funciones empresariales de sus organizaciones.

La evaluación del riesgo es uno de los componentes fundamentales de un proceso organizativo de gestión de riesgos, tal como se describe en la publicación especial NIST 800-39. Las evaluaciones de riesgo se usan para identificar, estimar y priorizar el riesgo para las operaciones organizacionales (es decir, misión, funciones, imagen y reputación), activos organizacionales, individuos, otras organizaciones, resultantes de la operación y uso de sistemas de información. El propósito de las evaluaciones de riesgo es informar a los que deben tomar decisiones y apoyar las respuestas de riesgo identificando: amenazas relevantes a las organizaciones o amenazas dirigidas a través de organizaciones contra otras organizaciones; vulnerabilidades tanto internas como externas a las organizaciones; impacto (es decir, daño) para las organizaciones que pueden ocurrir dado el potencial de amenazas que explotan las vulnerabilidades; Y probabilidad de que ocurra un daño. El resultado final es una determinación del riesgo (es decir, típicamente una función del grado de daño y probabilidad de daño que ocurre).

Las evaluaciones de riesgos pueden realizarse en los tres niveles de la jerarquía de gestión de riesgos, incluyendo Nivel 1 (nivel de organización), Nivel 2 (nivel de misión / proceso de negocio) y Nivel 3 (nivel de sistema de información). En las Etapas 1 y 2, las organizaciones utilizan evaluaciones de riesgo para evaluar, por

ejemplo, los riesgos sistémicos relacionados con la seguridad asociados a las actividades de gestión y gestión de la organización, los procesos de misión / negocio, la arquitectura empresarial o la financiación de programas de seguridad de la información. En el Nivel 3, las organizaciones usan evaluaciones de riesgo para apoyar más eficazmente la implementación del Marco de Gestión de Riesgo (es decir, categorización de seguridad, selección, implementación y evaluación del control de seguridad, sistema de información y autorización de control común).

## 2.5 NIST 800-44

En [6], la Publicación Especial NIST 800-44 se centra en los problemas de seguridad de los servidores Web, ya que son a menudo los hosts más atacados en las redes de las organizaciones, como resultado, es esencial asegurar los servidores web y la infraestructura de red que los soporta.

Las organizaciones deben implementar prácticas y controles de administración de seguridad apropiados para mantener y operar un servidor Web seguro.

Las prácticas de administración apropiadas son esenciales para operar y mantener un servidor Web seguro. Las prácticas de seguridad implican la identificación de los activos del sistema de información y desarrollo de documentación e implementación de políticas, normas, procedimientos y

directrices que ayuden a garantizar la confidencialidad, integridad y disponibilidad de los recursos del sistema de información. Para garantizar la seguridad de un servidor Web y la infraestructura de red de soporte, deben implementarse varias prácticas que se describen en la publicación NIST 800-44, como son:

• Política de seguridad del sistema de información de toda la Organización

• Control de configuración / cambio y gestión

• Evaluación y gestión de riesgos

• Configuraciones de software estandarizadas que satisfacen la política de seguridad del sistema de información

• Sensibilización y formación en materia de seguridad

• Planificación de contingencia, continuidad de operaciones y planificación de recuperación de desastres

• Certificación y acreditación.

Las organizaciones deben asegurarse de que los sistemas operativos del servidor Web se implementen, configuren y administren para satisfacer los requisitos de seguridad de la organización.

El primer paso para proteger un servidor Web es proteger el sistema operativo subyacente. La mayoría de los servidores Web disponibles operan en un sistema operativo de propósito general. Se pueden evitar muchos problemas de seguridad si los sistemas operativos subyacentes a los servidores Web están configurados adecuadamente. Las configuraciones predeterminadas de hardware y software son normalmente establecidas por los fabricantes para enfatizar características, funciones y facilidad de uso, a expensas de la seguridad. Debido a que los fabricantes no son conscientes de las necesidades de seguridad de cada organización, cada administrador del servidor Web debe configurar nuevos servidores para reflejar los requisitos de seguridad de su organización y reconfigurarlos conforme cambien esos requisitos. El uso de guías de configuración de seguridad o listas de comprobación puede ayudar a los administradores a asegurar los sistemas de manera consistente y eficiente.

Asegurar un sistema operativo inicialmente incluiría generalmente los siguientes pasos:

• Corregir y actualizar el sistema operativo

• Eliminar o inhabilitar servicios y aplicaciones innecesarias

• Configurar la autenticación del usuario del sistema operativo

• Configurar controles de recursos

• Instalar y configurar controles de seguridad adicionales

• Realizar pruebas de seguridad del sistema operativo.

Las organizaciones deben asegurarse de que la aplicación del servidor Web se implementa, configura y administra para cumplir con los requisitos de seguridad de la organización.

En muchos aspectos, la instalación y configuración seguras de la aplicación del servidor Web reflejarán el proceso del sistema operativo expuesto anteriormente. El principio general es instalar la cantidad mínima de servicios de servidor Web necesarios y eliminar cualquier vulnerabilidad conocida a través de parches o actualizaciones. Si el programa de instalación instala aplicaciones, servicios o secuencias de comandos innecesarias, deben quitarse Inmediatamente después de concluir el proceso de instalación. La seguridad de la aplicación del servidor Web generalmente incluiría los siguientes pasos:

• Actualizar la aplicación del servidor Web

• Eliminar o inhabilitar servicios, aplicaciones y contenido de muestra innecesarios

• Configurar la autenticación de usuario y los controles de acceso del servidor Web

• Configurar los controles de recursos del servidor Web

• Probar la seguridad de la aplicación del servidor web y del contenido Web.

Las organizaciones deben tomar medidas para garantizar que sólo el contenido apropiado se publica en un sitio Web.

Muchas agencias carecen de un proceso o política de publicación en la Web que determine qué tipo de información publicar públicamente, qué información publicar con acceso restringido y qué información no debe publicarse en ningún repositorio accesible al público. Esto es lamentable porque los sitios web son a menudo uno de los primeros lugares que las entidades maliciosas buscan información valiosa. Algunos ejemplos generalmente aceptados de lo que no se debe publicar o por lo menos deben ser cuidadosamente examinados y revisados antes de la publicación en un sitio web público incluyen:

• Información clasificada o exclusiva

• Información sobre la composición o preparación de materiales o toxinas peligrosas

• Información sensible relacionada con la seguridad nacional

• Registros médicos

• Las garantías físicas y de seguridad de información detalladas de una organización

• Detalles sobre la red de una organización y la infraestructura del sistema de información (por ejemplo, rangos de direcciones, convenciones de nombres, números de acceso)

• Información que especifica o implica vulnerabilidades de seguridad física

• Planes detallados, mapas, diagramas, fotografías aéreas y planos arquitectónicos de edificios organizativos, propiedades o instalaciones

•Toda información confidencial sobre personas, como información personal identificable (PII), que podría estar sujeta a leyes federales, estatales o, en algunos casos, internacionales.

## 2.6 NIST 800-45

En [7], podemos encontrar que el correo electrónico es quizás el sistema más utilizado para el intercambio de información comercial a través de Internet (o cualquier otra red informática). En el nivel más básico, el proceso de correo electrónico se puede dividir en dos componentes

principales: (1) servidores de correo, que son hosts que entregan, envían y almacenan correo electrónico; Y (2) clientes de correo, que interactúan con los usuarios y permiten a los usuarios leer, componer, enviar y almacenar correo electrónico. Esta Publicación trata los problemas de seguridad de los servidores de correo y los clientes de correo.

Los servidores de correo y las estaciones de trabajo de usuarios que ejecutan clientes de correo suelen ser atacados debido a que las tecnologías de computación y redes que subyacen al correo electrónico son omnipresentes y bien entendidas por muchos, los atacantes son capaces de desarrollar métodos de ataque para explotar las debilidades de seguridad. Los servidores de correo también están orientados porque ellos (y los servidores Web públicos) deben comunicarse en algún grado con terceros no confiables. Además, los clientes de correo han sido seleccionados como un medio eficaz de insertar malware en máquinas y de propagar este código a otras máquinas. Como resultado, los servidores de correo, los clientes de correo y la infraestructura de red que los soporta deben estar protegidos.

Las siguientes guías clave se recomiendan a los departamentos y agencias federales para mantener un servidor de correo seguro.

Las organizaciones deben planificar y abordar cuidadosamente los aspectos de seguridad del despliegue de un servidor de correo.

Dado que es mucho más difícil abordar la seguridad una vez que se hayan implementado, la seguridad debe ser considerada desde la etapa de planificación inicial. Es más probable que las organizaciones tomen decisiones sobre cómo configurar las computadoras de manera adecuada y consistente cuando desarrollan y utilizan un plan de implementación detallado y bien diseñado. Desarrollar un plan de este tipo apoyará a los administradores del servidor de correo en la toma de decisiones inevitables entre la usabilidad, el rendimiento y el riesgo.

A menudo, las organizaciones no toman en consideración los requisitos de recursos humanos tanto para las fases de despliegue como para las fases operativas del servidor de correo y la infraestructura de soporte. Las organizaciones deben abordar los siguientes puntos en un plan de despliegue:

• Tipos de personal necesarios (por ejemplo, administradores de sistemas y servidores de correo, administradores de red, oficiales de seguridad de sistemas de información)

• Habilidades y capacitación requeridas por el personal asignado

• Disponibilidad de personal

Las organizaciones deben implementar prácticas y controles de administración de seguridad apropiados al mantener y operar un servidor de correo seguro.

Las prácticas de administración apropiadas son esenciales para operar y mantener un servidor de correo seguro. Las prácticas de seguridad implican la identificación de los activos del sistema de información de una organización y el desarrollo, documentación e implementación de políticas, estándares, procedimientos y guías que ayuden a garantizar la confidencialidad, integridad y disponibilidad de los recursos del sistema de información.

Para garantizar la seguridad de un servidor de correo y la infraestructura de red de soporte, deben implementarse las siguientes prácticas:

• Política de seguridad del sistema de información de toda la Organización

• Configuración / control y gestión de cambios

• Evaluación y gestión de riesgos

• Configuraciones de software estandarizadas que satisfacen la política de seguridad del sistema de información

• Sensibilización y formación en materia de seguridad

• Contingencia, continuidad de operaciones y planificación de recuperación ante desastres

• Certificación y acreditación.

## 2.7 Política de Seguridad

En [8], según la Norma ISO 27001 en su sección 5.2 define que la alta dirección debe establecer una política de seguridad de la información que:

a) Sea adecuada al propósito de la organización

b) Incluya objetivos de seguridad de la información o proporcione el marco de referencia para el establecimiento de los objetivos de seguridad de la información.

c) Incluya compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información; e

d) Incluya el compromiso de mejora continua del sistema de gestión de seguridad de la información.

e) La política de seguridad de la información debe:

f) Estar disponible como información documentada;

g) Comunicarse dentro de la organización, y;

h) Estar disponible para las partes interesadas, según sea apropiado.

# CAPÍTULO 3

## LEVANTAMIENTO DE NECESIDADES

### 3.1 Organización

El área de sistemas se encarga del mantenimiento del centro de datos del centro de investigación y desarrollo de aplicativos para proyectos.

Actualmente cuenta con 2 roles: un desarrollador y un encargado de soporte y esto es liderado por el jefe de productos computacionales.

El puesto al que se reporta directamente es con el director del centro de investigación en el área administrativa.

*En la siguiente figura se presenta el Organigrama del Centro.*

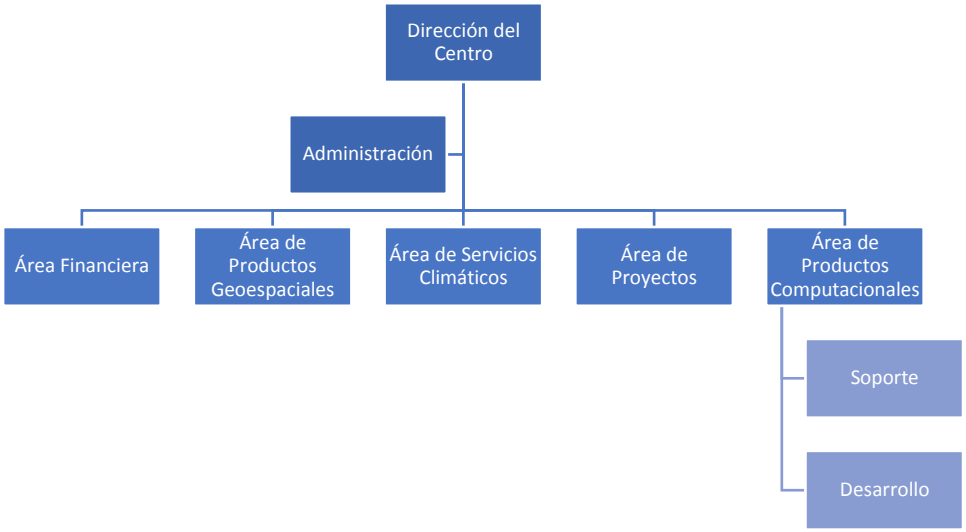


**Figura 3.1 Organigrama del CIIFEN.**

*Actividades que desempeña cada una de las personas del Centro.*

Director del Centro

• Supervisar el trabajo del Centro.

• Encargado de planificar, organizar, dirigir, controlar y supervisar las actividades administrativas financieras del Centro.

Jefe Financiero

• Encargado de planificar, organizar, dirigir, supervisar las actividades financieras del Centro.

• Encargado de planificar, organizar, dirigir, supervisar las actividades financieras de los proyectos que desarrolla el centro.

Asistente de Tributación

• Encargado de contabilidad y tributación del centro y los proyectos del centro.

Jefe de Productos Geoespaciales

• Encargado de planificar, organizar, dirigir, supervisar y ejecutar la parte técnica de proyectos que ejecuta el centro.

• Creación de mapas temáticos, plantillas de mapas y demás funciones dentro del área de cartografía digital orientado a ambiente.

Asistente de Productos Geoespaciales

• Creación de mapas temáticos, plantillas de mapas, modelación climática, investigación aplicada al clima y ambiente y demás funciones dentro del área de cartografía digital orientado a ambiente.

Secretaria

• Encargada de asistir al director del Centro.

• Encargada de logística de eventos, talleres y conferencias del Centro.

Jefe de Proyectos

• Encargado de dirigir, planificar y supervisar proyectos.

Operador Climático

• Encargado de la elaboración de boletines sobre clima.

• Investigación aplicada del área de clima.

• Ejecutor de componentes de proyectos en el área de clima.

• Modelación climática.

## 3.2 Procesos

*Actividades que desempeña cada una de las personas del área de sistemas.*

El jefe de productos computacionales es el encargado de mantener en funcionamiento el centro de datos del centro de datos.

Entre las actividades que realiza el jefe de productos computacionales están:

• Monitoreo de la generación del modelo climático WRF y su correcta publicación en el sitio web del centro regional del clima.

• Monitoreo de capacidad de almacenamiento de los servidores críticos del centro de investigación.

• Monitoreo de la capacidad de disco destinado a respaldo de los datos que produce el modelo climático WRF.

• Monitoreo de la disponibilidad de los sitios web que posee el centro.

• Monitoreo de la disponibilidad del servicio de internet en la oficina.

• Monitoreo del funcionamiento de los aplicativos desarrollados por los proyectos en los que fue participe el centro de investigación.

• Desarrollo de aplicativos a la medida para proyectos desarrollados por el centro de investigación.

• Creación de términos de referencia para contratación de nuevos consultores en el área informática.

• Administración de contratos con proveedores de tecnologías de información.

• Respaldo de información de los servidores.

• Monitoreo del funcionamiento de los servidores críticos del centro de investigación.

• Levantamiento de tickets de soporte.

• Actualizar el inventario.

• Actualizar la bitácora de préstamo de equipos.

• Adquisición de equipos para el centro de datos.

*Funciones externas al área de sistemas*

El proveedor externo de soporte de impresoras se encarga de realizar los siguientes servicios:

• Proveedor de equipos de impresión.

• Proveedor de insumos de impresión.

• Mantenimiento de impresoras.

• Resolución de incidentes de las impresoras.

El proveedor externo de soporte a equipos de computación y servidores se encarga de realizar los siguientes servicios:

• Resolución de incidentes de soporte de equipos de computación.

• Instalación de nuevos aplicativos en las estaciones de trabajo.

• Mantenimiento preventivo de estaciones de trabajo.

• Resoluciones de incidentes de nivel crítico en los servidores.

• Proveedor de equipos de computación.

*La siguiente tabla nos presenta el Inventario de procesos de negocio*

**Tabla 1 Inventario de Procesos de Negocio.**

| Proceso de Negocio | Nombre del Sistema | Lugar donde se encuentran los equipos | Instalaciones Propias o de | Proveedor del sistema | Equipo donde procesa el sistema | Sistema Operativo | Lenguaje Operativo | Base de datos | Fecha de inicio de operación del sistema |
|---|---|---|---|---|---|---|---|---|---|
| **Contable** | Sistema de administración contable | Centro de datos (Centro de Investigación) | Propias | Agrosoft | IBM ThinkCenter | Windows Server 2012 Foundation | Delphi | Microsoft sql server | 8 de enero del 2009 |
| **Contable por proyectos** | Sistema de administración contable por proyectos | Centro de datos (Centro de Investigación) | Propias | Software Sagitario | IBM ThinkCenter | Windows Server 2012 Foundation | Java | MYSQL | 12 septiembre del 2013 |
| **Sistema Base de datos Climática** | LACA &D | Centro de datos (Centro de Investigación) | Propias | KNMI - Netherlands | Dell Power Edge | Centos 5.6 | Php, c, fortrand | MYSQL | Mayo 2012 |
| **Desarrollo de proyectos ambienta-les** | Proyectos de Desarrollo Web | Centro de datos (Centro de Investigación), VPS's | Propias y de terce- ros | Consultorias y Propios | Dell Power Edge | CentOs 5.6 | PHP, Ruby, Python | MYSQL, POSTGRES | Mayo 2011 |
| **Adminis-tración** | Sistema biométrico de ingreso y salida de personal | Centro de datos (Centro de Investigación) | Propias | Propio | Hp Proliant ML350 | Ubuntu 12.01 | Java | MYSQL | Noviembre 2015 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Difusión** | Sistema de envió de boletines | Centro de datos (Centro de Investigación) | Propias | Propio | SUN Fire X2200 | Ubuntu 12.01 | Java | MYSQL | Mayo 2013 |
| **Difusión** | Manejador de Contenido (Sitios Web) | Hosting | De terceros | Propio | No aplica | Ubuntu 12.01 | PHP | MYSQL | Junio 2005 |
| **Clima** | Modelo WRF | Centro de datos (Centro de Investigación) | Propias | Consultor Externo | Hp Proliant ML350 | CentOs 6.5 | C, fortrand | No aplica | Agosto 2014 |
| **Clima** | Sistema de Visualización y generación de Imágenes Climáticas | Centro de datos (Centro de Investigación) y Hosting | Propias y de terce- ros | Propio y Consultor Externo | Hp Proliant ML350 | CentOs 6.5 | C, Fortrand, PHP | MYSQL | Julio 2013 |

**Prestación de Servicios por proveedores**

A continuación, presentamos una tabla para control de proveedores

**Tabla 2 Control de Proveedores.**

| Servicio Contratado | Empresa | Fecha de finalización del contrato | Indicadores del acuerdo de servicio | Responsable de Evaluar | Frecuencia de Evaluación del Nivel | Acuerdos de confidencialidad (Si/No) |
|---|---|---|---|---|---|---|
| Internet Dedicado (1) | Telconet | ago-16 | Porcentaje de Disponibilidad | Jefe de Productos Computacionales | Anual | Si |
| Internet Dedicado (2) | Telconet | feb-17 | Porcentaje de Disponibilidad | Jefe de Productos Computacionales | Anual | Si |
| Soporte de Equipos de Computación Y Servidores | Rayka Solutions | sep-17 | Tiempo de atención de incidentes | Jefe de Productos Computacionales | Semestral | No |
| Hosting para sitio web | Godaddy | Julio 2012 | Porcentaje de Disponibilidad | Jefe de Productos Computacionales | Anual | No |
| Servidor Virtual | Kimsufi | jul-14 | Porcentaje de Disponibilidad | Jefe de Productos Computacionales | Trimestral | No |

Información fuera de las instalaciones

El proveedor de soporte de Equipos de Computación y Servidores posee información de las IP’s que nos da el proveedor de internet.

Estrategia de continuidad de los proveedores.

El proveedor de soporte de Equipos de Computación y Servidores nos ofrece como estrategia de continuidad la disponibilidad de otro técnico, pero con grado de experticia inferior.

El proveedor de servicio de internet dedicado no nos ofrece ninguna estrategia de redundancia, nos ofrece una disponibilidad del servicio del 99,99% y revisión de incidente de disponibilidad en sitio en alrededor de una hora.

Acceso a sistemas o bases de datos por parte de proveedores

El proveedor de soporte de Equipos de Computación y Servidores posee acceso a todas las credenciales de todos los servidores.

El proveedor de soporte de Equipos de Computación y Servidores posee acceso a la cuenta de administración de las estaciones de trabajo.

El proveedor de soporte de Equipos de Computación y Servidores posee acceso a la cuenta de administración del sistema contable.

**Respaldos de Información**

**Procedimientos de respaldo de Información**

Actualmente se cuenta con respaldo de la base de datos MySQL y aplicativos que se encuentra en el servidor Gateway, también se realizan los respaldos de la información de cada uno de los funcionarios del centro.

**Respaldo de base de datos**

MYSQL en Servidor Gateway

- El equipo donde se encuentra el aplicativo es el Dell Power Edge 2950 que tiene el nombre de Servidor Gateway.

- La ubicación se encuentra en la siguiente carpeta: /var/mysql

- El servidor se encuentra en el rack del centro de datos del centro de investigación y es el segundo servidor en sentido de arriba para abajo, el disco externo de respaldos se encuentra conectado a este servidor.

- Hay un script programado en bash que se ejecuta mensualmente que copia la información de la ubicación, la comprime y le asigna la fecha actual y la manda al disco externo.

- El responsable de realizar este respaldo es el Jefe de Productos Computacionales.

MYSQL en Hosting

- El equipo donde se encuentra el aplicativo es en un servidor virtual del hosting.

- La ubicación se encuentra en un servidor especializado de bases de datos del hosting, pero cuando se hace el procedimiento de respaldo la ubicación es la siguiente: /home/content/27/10028227/html/databases

- El servidor se encuentra en un servidor del proveedor de servicio de hosting godaddy.com.

- En la consola de administración se presiona el botón dump de cada una de las bases de datos en el servidor de manera mensual se realiza una descarga del contenido de esa carpeta de manera manual.

- El responsable de realizar este respaldo es el Jefe de Productos Computacionales.

**Respaldo de Archivos (Productos Computacionales)**

Productos Finales Generados por el Modelo Climático WRF

- El equipo es un servidor dedicado a realizar esta tarea.

- La ubicación es /home/ciifen/WRF.

- El servidor se encuentra en el centro de datos.

- Hay un script programado en el cron del servidor y automáticamente manda al servidor de respaldo.

- El responsable de realizar este respaldo es el Jefe de Productos Computacionales.

Imágenes y Animaciones Climáticas

- El equipo es un servidor dedicado a realizar esta tarea.

- La ubicación es /home/ciifen/WRF.

- El servidor se encuentra en el centro de datos.

- Hay un script programado en el cron del servidor y automáticamente manda al servidor de respaldo.

- El responsable de realizar este respaldo es el Jefe de Productos Computacionales.

**Respaldo de Aplicativos**

Latin American Climate Assesment and Dataset – LACA&D

- El equipo donde se encuentra el aplicativo es el Dell Power Edge 2950 que tiene el nombre de Servidor Gateway.

- La ubicación se encuentra en la siguiente carpeta: /data/ciifen

- El servidor se encuentra en el rack del centro de datos del centro de investigación y es el segundo servidor en sentido de arriba para abajo, el disco externo de respaldos se encuentra conectado a este servidor.

- Hay un script programado en bash que se ejecuta mensualmente que copia la información de la ubicación, la comprime y le asigna la fecha actual y la manda al disco externo.

- El responsable de configurar y dar mantenimiento a este respaldo es el Jefe de Productos Computacionales.

Aplicaciones web de proyectos pasados

- El equipo donde se encuentra el aplicativo es el Dell Power Edge 2950 que tiene el nombre de Servidor Gateway.

- La ubicación se encuentra en la siguiente carpeta: /var/www

- El servidor se encuentra en el rack del centro de datos del centro de investigación y es el segundo servidor en sentido de arriba para abajo, el disco externo de respaldos se encuentra conectado a este servidor.

- Hay un script programado en bash que se ejecuta mensualmente que copia la información de la ubicación, la comprime y le asigna la fecha actual y la manda al disco externo.

- El responsable de configurar y dar mantenimiento a este respaldo es el Jefe de Productos Computacionales.

Sitio Web

- El equipo donde se encuentra el aplicativo es en un servidor virtual del hosting.

- La ubicación se encuentra en la siguiente carpeta: /home/content/27/10028227/html

- El servidor se encuentra en un servidor del proveedor de servicio de hosting godaddy.com.

- Mensualmente se realiza una descarga del contenido de esa carpeta de manera manual.

- El responsable de configurar y dar mantenimiento a este respaldo es el Jefe de Productos Computacionales.

Aplicaciones ofimáticas, de uso especializado y sistemas operativos

- El equipo donde se encuentra la estación de trabajo PROD-COMP.

- La ubicación se encuentra en la siguiente carpeta: D:/instaladores/

- El equipo se encuentra en el centro de datos.

- Hay una carpeta que contiene los instaladores de respaldo de las aplicaciones ofimáticas, de uso especializado y sistemas operativos.

- El responsable de configurar y dar mantenimiento a este respaldo es el Jefe de Productos Computacionales.

**Respaldo de Información de Usuarios**

- El equipo es cada una de las estaciones de trabajo de cada funcionario del centro.

- La ubicación varía de acuerdo a la criticidad de la información que maneja el funcionario, pero en general es la carpeta de mis documentos y de allí el funcionario adiciona las carpetas que considere críticas para realizar la configuración del respaldo.

- El equipo es cada una de las estaciones de trabajo de cada funcionario del centro.

- Hay un script programado con extensión .bat que se ejecuta diariamente de manera automática en la estación de trabajo que copia la información de las ubicaciones y la manda al servidor de respaldo.

- El responsable de configurar y dar soporte a estos respaldos es Rayka solutions.

La siguiente tabla presenta información sobre el almacenamiento de respaldos

**Tabla 3 Almacenamiento de respaldos.**

| **Responsable: Jefe de Productos Computacionales** | | | | | | |
|---|---|---|---|---|---|---|
| **Nombre del sistema, herramienta, base de datos, sistema operativo** | Tipo de Información respaldada | Frecuencia | Medio de almacenamiento | Lugar de resguardo | Ubicación | Fecha |
| **MYSQL en Servidor Gateway** | Base de datos | mensual | Disco Externo | Rack | Centro de Computo | 1 de cada mes |
| **MYSQL en Hosting** | Base de datos | mensual | Estación de trabajo PROD-COMP | Edificio Matriz | Centro de Computo | 1 de cada mes |
| **LACA&D** | Programas | mensual | Disco Externo | Rack | Centro de Computo | 1 de cada mes |
| **Aplicaciones web de proyectos pasados** | Programas | mensual | Disco Externo | Rack | Centro de Computo | 1 de cada mes |
| **Sitio Web** | Programas | mensual | Estación de trabajo PROD-COMP | Edificio Matriz | Centro de Computo | 1 de cada mes |
| **Aplicaciones Ofimáticas y Sistemas Operativos** | Configuración de Sistemas y Programas | Progresivo | CD, Archivos en PROD-COMP | Estante | Oficina de Sistemas | progresivo |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Excel, Claves** | Claves de todos los sistemas | Progresivo | Estación de trabajo PROD-COMP | Edificio Matriz | Centro de Computo | progresivo |
| **Información de usuarios** | Archivos de funcionarios | diaria | Servidor de Base de Datos | Edificio Matriz | Centro de Computo | diario |

**Procedimiento de recuperación de respaldos**

**Procedimiento de recuperación de bases de datos**

De manera general el respaldo se comprime en un archivo con extensión tar para ahorrar espacio. Los pasos para recuperar información de respaldos son los siguientes:

• El archivo de respaldo se extrae del medio de respaldo a otro equipo con capacidad para albergar el respaldo descomprimido.

• Se descomprime el archivo.

• Se revisa la información que se necesita extraer del respaldo.

• Se remplaza la información del respaldo en la base de datos en desarrollo.

• Se prueba que el sistema en producción funcione con la base de datos en desarrollo.

• Se realiza un respaldo de la base de datos corrupta o que se va a cambiar.

• Se reemplaza el respaldo de la base de datos de desarrollo en la base de datos de producción.

• Se borra el respaldo extraído.

**Procedimiento de recuperación de archivos**

Los pasos para recuperar información de respaldos son los siguientes:

• Se revisa la fecha de la cual se quiere el respaldo.

• Se revisa la información que se necesita extraer del respaldo.

• Se remplaza la información del respaldo en el sistema en producción.

• Se borra el respaldo extraído.

**Procedimiento de recuperación de aplicativos**

De manera general el respaldo se comprime en un archivo con extensión tar para ahorrar espacio. Los pasos para recuperar información de respaldos son los siguientes:

• El archivo de respaldo se extrae del medio de respaldo a otro equipo con capacidad para albergar el respaldo descomprimido.

• Se descomprime el archivo.

• Se revisa la información que se necesita extraer del respaldo.

• Se remplaza la información del respaldo en el sistema en producción.

• Se borra el respaldo extraído.

**Procedimiento para recuperación de respaldos de información de usuarios**

Los pasos para recuperar información de respaldos son los siguientes:

• Se revisa la información que se necesita extraer del respaldo.

• Se extrae el respaldo.

## Listado de procesos del departamento de tecnologías de información.

Servicios prestados actualmente por el área de sistemas.

**Inventario de Equipos.**

• Se realiza una revisión anual del inventario de equipos.

• Se realiza ingreso de Equipos al inventario.

• Se realiza salida por préstamo de Equipo.

• Se realiza ingreso por préstamo de Equipo.

**Respaldo**.

• Cada semana de manera automática el servidor Gateway produce un respaldo de las aplicaciones web que se encuentran en la ubicación /var/www/html.

• De manera diaria se realiza un respaldo incremental de los equipos de cada una de las diferentes áreas.

**Desarrollo de Software.**

• Desarrollo de aplicativos webs para proyectos ambientales que se encuentra desarrollando la institución. Se desarrolla en conjunto con el área de GIS.

**Resolución de Incidentes de Soporte a Usuarios**.

• Administración de contratos y Fiscalización de Proyectos.

• Administración de contratos con servicio de proveedor de internet.

• Mantenimiento de UPS de Contingencia.

• Administración de contrato de soporte a usuarios y mantenimiento de servidores.

• Fiscalización de contratos de desarrollo de proyectos.

• Operaciones.

## 3.3 Infraestructura.

Los equipos de computación y servidores se encuentran en el centro de cómputo que está ubicado en el edificio principal del centro.

### 3.3.1 Requisitos mínimos de las instalaciones

El centro de datos cuenta con:

- 2 aires acondicionados Split de 12000 BTU.
- UPS delta 10kVA.
- Sistema de detección de humo.
- Sistema de extinción de incendios.

### 3.3.2 Enlaces de comunicación

**Tabla 4 Enlaces de Comunicación.**

| Tipo de Enlace | Ancho de Banda | Proveedor |
|---|---|---|
| Fibra Óptica | 1 mbps | Telconet |
| Fibra Óptica | 1 mbps | Telconet |

### 3.3.3 Distribución física

Actualmente el centro tiene dispuesta la infraestructura física de la siguiente forma:

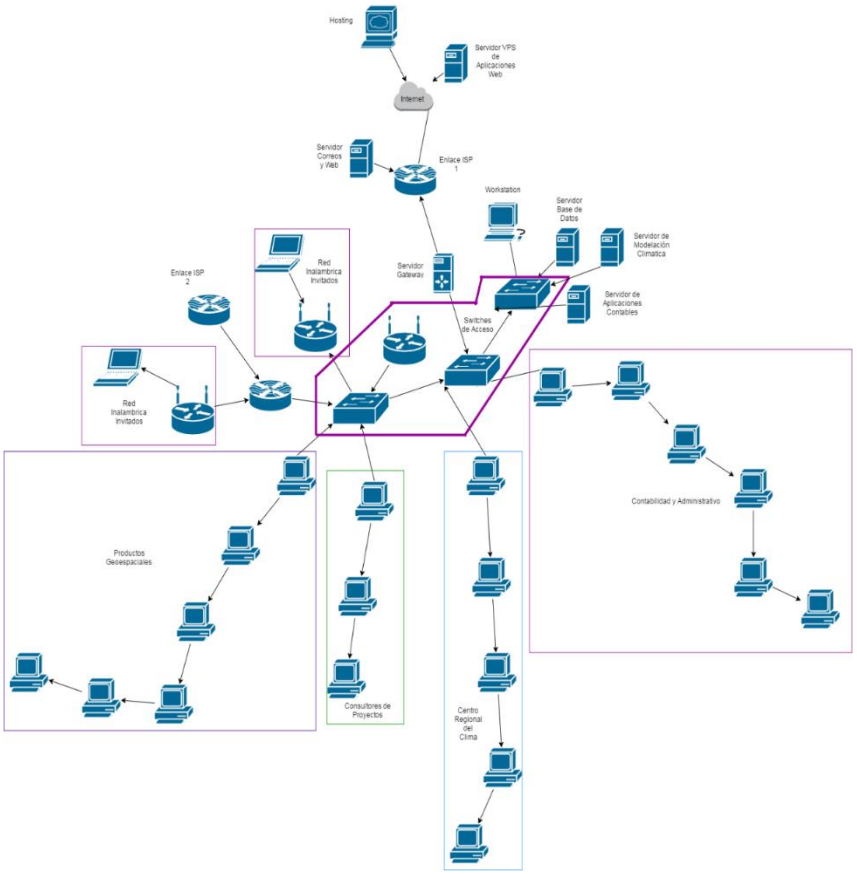


**Figura 3.2 Esquema de la Infraestructura Física de TI del Centro.**

Servidores:

1 servidor de Gateway Dell Power Edge.

1 servidor Base de Datos y Respaldos Dell Power Edge.

1 Servidor Envió de Correos Masivo y Web Server.

1 servidor para aplicaciones Contables.

1 servidor de modelación climática.

1 servidor VPS.

1 hosting web.

Estaciones de Trabajo:

Consultores de Proyectos - 3 computadores personales.

Otra y USAID área - 3 computadores personales.

Área de Productos Geoespaciales - 3 computadores personales y un servidor de archivos Workstation.

Área de Contabilidad y Administración - 3 computadores personales y 1 laptop

Dirección – 1 computador personal.

Secretaria – 1 computador personal.

Centro Regional del Clima 5 computadores personales.

Sala de Sesiones - 1 router inalámbrico.

Equipos de Redes:

Área de Servidores - 3 switches de 24 puertos en uso.

Centro Regional del Clima - 1 switch de 6 puertos.

Área de Productos Geoespaciales - 1 switch de 6 puertos.

Área de Contabilidad y Administración - 1 switch de 6 puertos.

Sala de Sesiones - 1 router inalámbrico.

### 3.3.4 Distribución lógica

La distribución lógica del centro se encuentra dispuesta en una sola red de datos con la siguiente información sobre la red:

| Red | Mascara | Puerta de Salida |
|---|---|---|
| 172.16.99.0 | 255.255.255.0 | 172.16.99.1 |

## 3.4 Software.

El centro promueve el uso de software libre, no obstante, también se utiliza software licenciado. Los aplicativos de software utilizado por el centro es el presentado a continuación:

**Tabla 5 Aplicativos de Software Usados en el Centro.**

| Tipo | Software |
|---|---|
| **Sistemas Operativos** | Microsoft Window 7, 8, 8.1, 10<br>Microsoft Windows Server 2012 Foundation (Web Server Edition)<br>Ubuntu 10,12.01<br>CentOs 5.6, 6.5 |
| **Ofimática** | Microsoft Office 2007,2013,2016 |
| **Organizador Personal** | Microsoft Outlook, Mozilla ThunderBird |
| **Navegador Web** | Google Chrome, Mozilla Firefox, Internet Explorer |
| **Software Especializado** | Esri ArcGIS 10.1, ArMap 10.1<br>ErDas, IDRISI, Open GRADS, SURFER 13 |
| **Sistema Contable** | Agrosoft, Software Sagitario |

A continuación, se detalla el software de desarrollo propio que funciona actualmente en el centro:

**Tabla 6 Software desarrollado en el Centro.**

| Nombre del Sistema | Lugar donde se encuentran los equipos | Instalaciones Propias o de terceros | Proveedor del sistema | Equipo donde procesa el sistema | Sistema Operativo | Lenguaje Operativo | Base de datos | Fecha de inicio de operación del sistema |
|---|---|---|---|---|---|---|---|---|
| **LACA&D** | Centro de datos (Centro de Investigación) | Propias | KNMI-Netherlands | Dell Power Edge | Centos 5.6 | Php, c, fortrand | MYSQL | Mayo 2012 |
| **Proyectos de Desarrollo Web** | Centro de datos (Centro de Investigación), VPS's | Propias y de terce-ros | Consultorias y Propios | Dell Power Edge | CentOs 5.6 | PHP, Ruby, Python | MYSQL, POSTGRES | Mayo 2011 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Sistema biométrico de ingreso y salida de personal** | Centro de datos (Centro de Investigación) | Propias | Propio | Hp Proliant ML350 | Ubuntu 12.01 | Java | MYSQL | Noviembre 2015 |
| **Sistema de envió de boletines** | Centro de datos (Centro de Investigación) | Propias | Propio | SUN Fire X2200 | Ubuntu 12.01 | Java | MYSQL | Mayo 2013 |
| **Manejador de Contenido (Sitios Web)** | Hosting | De terceros | Propio | No aplica | Ubuntu 12.01 | PHP | MYSQL | Junio 2005 |

## 3.5 Seguridades.

### 3.5.1 Control de acceso a los aplicativos

**Perfiles de usuario**

Actualmente existen 2 perfiles de usuario en el centro:

Administrador: Es el súper usuario el usuario de sistemas para dar soporte, el usuario de sistemas para los cambios de sistemas tanto web como de escritorio.

Técnico: Es el funcionario del centro que desea realizar su trabajo en alguna estación de trabajo y usar algún sistema para

realizar una operación específica, dependiendo del rol que tengan.

#### 3.5.1.1 Procedimientos de alta de los usuarios

**Alta en correo electrónico**

**Procedimiento:**

El usuario o su jefe inmediato solicita que se le cree una cuenta de correo electrónico.

Se espera autorización del jefe inmediato para la creación de dicha cuenta.

La persona de sistemas responsable crea el usuario en el servidor de correo.

Se le entrega los accesos al correo electrónico.

Se le enseña a ingresar desde la plataforma web.

Se le envía un correo de confirmación con el nuevo correo institucional a él y a su equipo de trabajo.

Se le enseña a usar la plataforma online de acceso al correo electrónico de la institución.

Se le configura el Outlook o programa de escritorio para recepción de correo electrónico (Opcional).

Responsable:

La persona responsable es el Jefe de Productos Computacionales.

Medio de solicitud del alta:

La solicitud de alta se la realiza por medio de correo electrónico.

**Procedimiento de entrega de usuario y contraseña:**

La persona de sistemas procede a entregarle los accesos en un medio físico y se lo capacita para su acceso a la plataforma online y al programa de recepción de correo de escritorio que tenga en su estación de trabajo.

**Alta en bases de datos para desarrollo**

**Procedimiento**:

El desarrollador o su jefe inmediato solicita que se le cree una cuenta de bases de datos.

Se espera autorización del jefe inmediato para la creación de dicha cuenta.

La persona de sistemas responsable crea el usuario en el servidor de bases de datos.

Se le entrega los accesos a la base de datos al desarrollador.

Se verifica la conexión del equipo de desarrollo con la base de datos.

Se le envía un correo de confirmación de la creación del usuario a el usuario y a su jefe inmediato.

Responsable:

La persona responsable es el Jefe de Productos Computacionales.

Medio de solicitud del alta:

La solicitud de alta se la realiza por medio de correo electrónico.

**Procedimiento de entrega de usuario y contraseña:**

La persona de sistemas procede a entregarle los accesos en un medio físico y se respalda en la bitácora de claves del centro de cómputo.

**Alta en servidores**

**Procedimiento**:

El usuario o su jefe inmediato solicita que se le cree una cuenta de acceso a servidor.

Se espera autorización del jefe inmediato para la creación de dicha cuenta.

La persona de sistemas responsable crea el usuario en el servidor.

Se le entrega los accesos al servidor al usuario.

Se verifica la conexión del equipo con el servidor.

Se le envía un correo de confirmación de la creación del usuario a el usuario y a su jefe inmediato.

Responsable:

La persona responsable es el Jefe de Productos Computacionales.

Medio de solicitud del alta:

La solicitud de alta se la realiza por medio de correo electrónico.

Procedimiento de entrega de usuario y contraseña:

La persona de sistemas procede a entregarle los accesos en un medio físico y se respalda en la bitácora de claves del centro de cómputo.

**Alta en aplicativos**

**Procedimiento**:

El usuario o su jefe inmediato solicita que se le cree una cuenta de acceso a una aplicación.

Se espera autorización del jefe inmediato para la creación de dicha cuenta.

La persona de sistemas responsable crea el usuario en el aplicativo.

Se le entrega los accesos al aplicativo al usuario.

Se verifica la conexión del equipo con el aplicativo.

Se le envía un correo de confirmación de la creación del usuario en el aplicativo al usuario y a su jefe inmediato.

Responsable:

La persona responsable es el Jefe de Productos Computacionales.

Medio de solicitud del alta:

La solicitud de alta se la realiza por medio de correo electrónico.

Procedimiento de entrega de usuario y contraseña:

La persona de sistemas procede a entregarle los accesos en un medio físico y se respalda esta información en la bitácora de claves del centro de cómputo.

#### 3.5.1.2 Procedimiento de Baja de los Usuarios

**Baja en correo electrónico**

**Procedimiento:**

El usuario o su jefe inmediato solicitan que se le borre una cuenta de correo electrónico.

Se espera autorización del jefe inmediato para la creación de dicha cuenta.

La persona de sistemas responsable desactiva la cuenta del usuario en el servidor de correo por 3 meses dependiendo del rol del usuario.

Se re direcciona el tráfico de esa cuenta a una cuenta de usuario de la misma área del usuario dado de baja.

Se borra la cuenta del servidor de correo.

Responsable:

La persona responsable es el Jefe de Productos Computacionales.

Medio de solicitud de baja:

La solicitud de alta se la realiza por medio de correo electrónico.

Procedimiento de entrega de usuario y contraseña:

El usuario procede a entregarle los accesos en un medio físico y se verifica en la bitácora de claves del centro de cómputo.

**Baja en servidores**

**Procedimiento:**

El usuario, el jefe de productos computacionales o su jefe inmediato solicita que se le borre una cuenta del servidor.

Se espera autorización del jefe inmediato para la creación de dicha cuenta.

Se borra la cuenta del servidor.

Responsable:

La persona responsable es el Jefe de Productos Computacionales.

Medio de solicitud de baja:

La solicitud de alta se la realiza por medio de correo electrónico.

Procedimiento de entrega de usuario y contraseña:

El usuario procede a entregarle los accesos en un medio físico y se verifica en la bitácora de claves del centro de cómputo.

**Baja en aplicativos**

**Procedimiento:**

El usuario, el jefe de productos computacionales o su jefe inmediato solicita que se le borre una cuenta del aplicativo.

Se espera autorización del jefe inmediato para la creación de dicha cuenta.

Se cambia la contraseña a ese usuario.

Se verifica que la desactivación de esa cuenta no interfiera con la integridad de los datos.

Se desactiva la cuenta del aplicativo.

Responsable:

La persona responsable es el Jefe de Productos Computacionales.

Medio de solicitud de baja:

La solicitud de alta se la realiza por medio de correo electrónico.

**Procedimiento de entrega de usuario y contraseña**:

El usuario procede a entregarle los accesos en un medio físico y se verifica en la bitácora de claves del centro de cómputo.

**Procedimientos para asignar o modificar un perfil a un usuario de acuerdo a sus funciones**

**Procedimiento:**

El usuario, el jefe de productos computacionales o su jefe inmediato solicitan que se le agreguen, quiten funciones.

Se espera autorización del jefe inmediato para la modificación de funciones.

Se revisa que funciones serán agregadas o quitadas.

Se realiza el cambio.

Responsable:

La persona responsable es el Jefe de Productos Computacionales.

**Procedimientos para el restablecimiento de cuentas bloqueadas o contraseñas olvidadas**

**Procedimiento:**

El usuario, el jefe de productos computacionales o su jefe inmediato solicita el restablecimiento de cuenta.

Se espera autorización del jefe inmediato para la creación de dicha cuenta.

Se cambia la contraseña a ese usuario.

Responsable:

La persona responsable es el Jefe de Productos Computacionales.

### 3.5.2 Características de las contraseñas de acceso de los sistemas

**Tabla 7 Características de las Contraseñas de los Sistemas.**

| Aplicación o base de datos | Longitud Mínima | Composición de contraseña | Periodo de Rotación de Contraseña | Intentos Fallidos | Tiempo de Conexión | Cifrado de Contraseña |
|---|---|---|---|---|---|---|
| Sistema Contable | 6 caracteres | Letras y números | nunca | No tiene configurado | nunca | MD5 |
| Correo electrónico | 6 caracteres | Letras números y caracteres especiales | nunca | No tiene configurado | nunca | MD5 |
| Manejador de Contenido (Sitio Web) | 6 caracteres | Letras números y caracteres especiales | nunca | No tiene configurado | nunca | MD5 |
| Sistema de envió de boletines | 6 caracteres | Letras números y caracteres especiales | nunca | No tiene configurado | nunca | MD5 |
| Geoportal-BID | 6 caracteres | Letras números y caracteres especiales | nunca | No tiene configurado | nunca | MD5 |
| Proyectos de desarrollo web | 6 caracteres | Letras números y caracteres especiales | nunca | No tiene configurado | nunca | MD5 |
| Sistema biométrico de ingreso y salida de personal | 6 caracteres | Letras números y caracteres especiales | nunca | No tiene configurado | nunca | MD5 |

### 3.5.3 Políticas de control de acceso, usuarios finales y administradores de sistemas

- Todas las estaciones de trabajo Windows están configuradas con un mismo usuario administrador.

- El operador de soporte es la persona responsable por el acceso de la clave de administrador en cada una de las estaciones de trabajo Windows.
- Todos los equipos deben de tener un usuario y contraseña para el usuario aparte de la cuenta de administrador.
- El Jefe de Productos Computacionales es la persona responsable de administrar los accesos a las aplicaciones.
- La navegación por internet está controlada mediante proxy.
- La petición de accesos a servidor de archivos externos se realiza de acuerdo a autorización del director o jefe de área.

### 3.5.4 Cuentas con mayores privilegios

**Tabla 8 Detalle de Cuentas con Privilegios.**

| Aplicación o base de datos | Nombre y puesto del responsable de la cuenta | Nombre de la cuenta | Perfil de la cuenta | Actividades Realizadas con la cuenta |
|---|---|---|---|---|
| Base de datos climática | Jefe de Productos Computacionales | root | Super administrador | Respaldo de la base de datos. |

| | | | | |
|---|---|---|---|---|
| Base de datos - LACA&D | Jefe de Productos Computacionales | SA | Super administrador | Respaldo de la base de datos.<br>Ingreso de datos a la base de datos. |
| Base de datos – sistema biométrico de ingreso y salida de personal | Consultor externo | root | Super administrador | Respaldo de la base de datos.<br>Modificación de datos a la base de datos |
| Base de datos - hosting | Jefe de Productos Computacionales | Cada base de datos tiene su propia cuenta de administrador en el hosting | Super administrador | Respaldo de la base de datos.<br>Modificación de datos erróneo.<br>Depuración de la base de datos. |
| Manejador de Contenido (Sitio Web) | Jefe de Productos Computacionales | administrator | Super administrador | Cambios en configuración del aplicativo.<br>Ingreso, modificación y eliminación de componentes del sitio. |
| Sistema de envió de boletines | Jefe de Productos Computacionales | administrator | Super administrador | Cambios en configuración del aplicativo. |
| Geoportal- BID | Jefe de Productos Computacionales | administrador | Super administrador | Cambios en configuración del aplicativo.<br>Ingreso, modificación y eliminación de contenido del sitio. |
| Proyectos de desarrollo web | Jefe de Productos Computacionales | administrator | Super administrador | Cambios en configuración del aplicativo. |
| Sistema biométrico de ingreso y salida de personal | Jefe de Productos Computacionales | administrator | Super administrador | Cambios en configuración del aplicativo. |

### 3.5.5 Infraestructura de Seguridad

#### 3.5.5.1 Seguridad Física

El centro de datos del centro se encuentra en una oficina a la cual no tienen acceso todos los funcionarios del centro. Esta oficina esta resguardada bajo una puerta cuyo acceso es restringido solo al personal del área de sistemas.

#### 3.5.5.2 Seguridad Lógica

A nivel de servidores se tiene instalado diferentes versiones de cortafuegos, pero se encuentran entre estas versiones de iptables para los servidores Linux y ufw para los servidores de distribución Ubuntu.

Para filtrado de tráfico web se tiene instalado “Squid” pero actualmente solo funciona como invisible y no regula el tráfico de las estaciones de trabajo del centro. Se generan reportes del tráfico de las estaciones de trabajo mediante “Squid sarg”.

El centro tiene instalado en las estaciones de trabajo los siguientes antivirus y antimalware:

- Avast

- Norton Internet Security
- Cómodo personal firewall y antimalware.

# CAPÍTULO 4

## ANÁLISIS Y DISEÑO DEL ESQUEMA DE SEGURIDAD DE UN CENTRO DE INVESTIGACIÓN

### 4.1 Identificación del Proceso Central.

Para la definición del proceso central de la empresa se realizó una reunión con miembros del Centro de Investigación del área administrativa y del departamento de tecnologías de información en el cual se llegó a la conclusión de que estos son los procesos más críticos del centro:

- Proceso de compras y adquisiciones.
- Proceso de desarrollo de proyectos.
- Proceso de envío masivo de boletines por correo electrónico.

De estos 3 procesos se decidió mediante reunión con miembros del centro de investigación que el proceso central y el más crítico es el

proceso de envío masivo de boletines porque es el que si no se realiza estarían dejando de cumplir la misión y el objetivo por el cual funciona el centro de investigación.

## 4.2 Identificación de los activos del proceso central

El proceso de envío de correo consiste en el envío de un correo electrónico masivo 4 veces por mes con un enlace a el sitio web en el cual se encuentra el boletín

El proceso de envío de correo masivo de boletines está definido de la siguiente forma

- Sistema de envío de correo masivo de boletines.
- Servidor de Aplicaciones Web y Base de datos.
- Servidor Gateway.
- Servidor de Correos.
- Servidor Web.
- Estación de Trabajo.

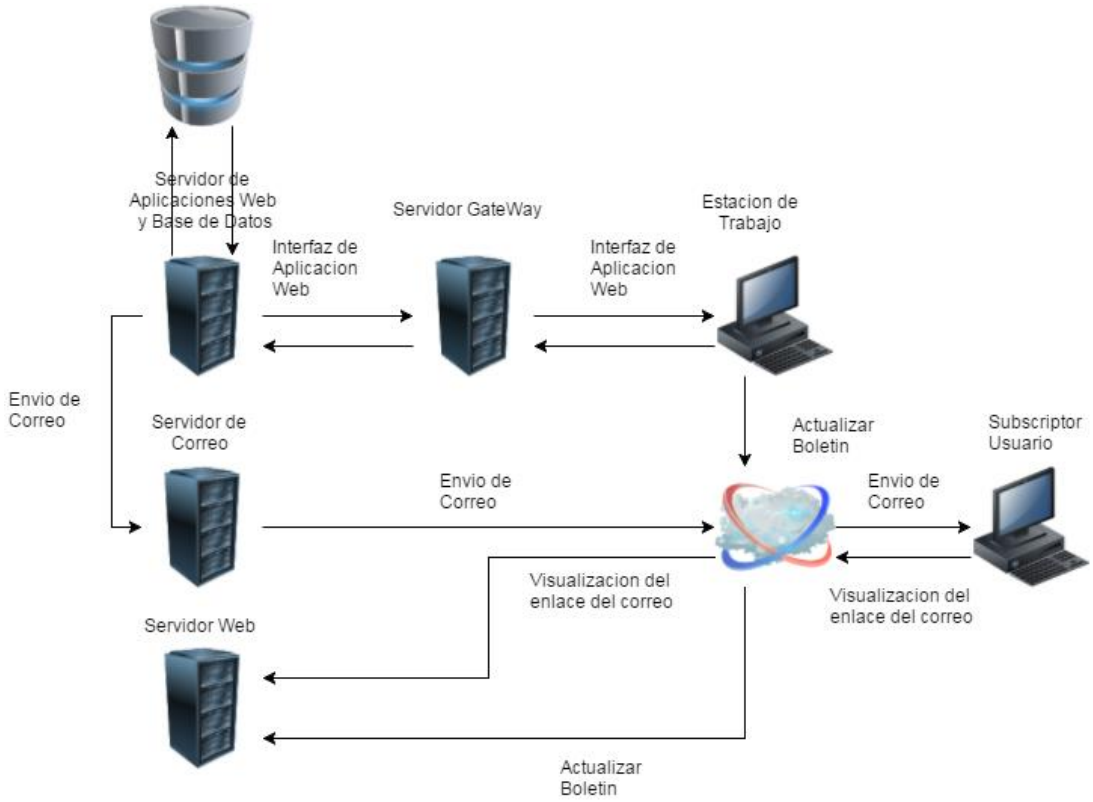


**Figura 4.1 Esquema del Proceso de Envío de Boletines.**

## 4.3 Clasificación y categorización de activos del proceso central.

**Tabla 9 Clasificación y categorización del Proceso Central.**

| **Inventario del sistema de TI y documento de definición** | | | |
|---|---|---|---|
| **I. Identificación y propiedad del sistema de TI** | | | |
| **ID del sistema de TI** | **SECM** | **Nombre común del sistema de TI** | **Sistema de Envió de Correos Masivos** |
| **Propiedad de** | **Centro de Investigación** | | |

| | | | |
|---|---|---|---|
| **Localización física** | **Oficina Principal, Escobedo # 1204 y 9 de octubre, GYE EC** | | |
| **Función Empresarial importante** | **Envió de información climática a tomadores de decisiones y organismos gubernamentales. Se envían 4 boletines diferentes al mes cada semana.**<br>• **Boletín del CI. se publica el primer día del mes. Este servicio de información provee a los usuarios una síntesis que analiza las condiciones oceanográficas y los efectos climáticos relacionados con los fenómenos El Niño y La Niña, desde una perspectiva regional del Pacífico Oriental.**<br>• **Boletín Análisis del Pacífico Oriental. Se publica el día 10 del mes. Este producto provee un análisis muy resumido de las principales condiciones oceanográficas en el Pacífico oriental, revisando el estado presente y estimado del mar tanto en superficie como sub-superficialmente. Integra información satelital y datos provenientes de boyas fijas y a la deriva. De igual manera compila los más relevantes pronósticos de temperatura del mar, para proveer a los usuarios de información entendible y aplicable en el área marino costera.**<br>• **Pronóstico Estacional. Se publica el día 15 del mes. Este producto es útil para tener una referencia de más largo plazo en el tiempo, pero es necesario aclarar que no consideran eventos extremos puntuales y de corta duración que puedan ocurrir en los distintos países. Este producto se está desarrollando a nivel nacional para lo cual la fuente primaria de información son los Servicios Meteorológicos Nacionales.**<br>• **d. Diagnóstico del ENOS. Se publica el día 25 del mes. En este boletín se presenta una revisión global de las condiciones oceánicas y atmosféricas del Pacífico Tropical relacionadas con el evento ENOS y las perspectivas de evolución futura conforme a la predicción de modelos.** | | |
| **Dueño de sistema Número de teléfono** | **2514770** | **Número de teléfono Administrador de sistema(s)** | **2514770-105** |

| | | | | |
|---|---|---|---|---|
| **Dueño de dato(s) Número de teléfono (s)** | **2514770** | | **Número de teléfono(s) Dato Custodian(s)** | **2514770-105** |
| **Otra Información Pertinente** | | | | |
| **II. Alcance de sistema y Componentes TI** | | | | |
| **Descripción de sistema y Componentes TI** | **El sistema es un aplicativo de entorno web diseñado para que el operador climático pueda enviar el boletín del clima una vez que él lo termine de crear envíe mediante correo electrónico a un listado de suscriptores que se encuentra en una base de datos local, un enlace al sitio web en el cual se encuentra colocado el boletín en formato PDF correspondiente a cada uno de los diferentes boletines.<br>El sistema se encuentra desarrollado en lenguaje de programación Java con el uso del marco de referencia de desarrollo Spring.<br>Los componentes de arquitectura del sistema son los siguientes:<br>Servidor de Aplicaciones, Servidor de Correos, Servidor web, Hosting y la máquina de escritorio del Operador.** | | | |
| **Interfaces de sistema TI** | **La interfaz que tiene el sistema es el sitio web y el aplicativo de entorno web desarrollado en Java.** | | | |
| **Límite de sistema TI** | **El aplicativo está desarrollado solamente para enviar correos electrónicos a el listado de suscriptores.** | | | |
| **III. Interconexiones de sistema TI** | | | | |
| **Agencia u Organización** | **Nombre de sistema TI** | **ID del sistema de TI** | **Dueño de sistema TI** | **Seguridad de Interconexión Acuerdo de la seguridad** |

| | | | | |
|---|---|---|---|---|
| **CI** | **SECM** | **SECM** | **Productos Computacionales** | **Ingreso al sistema mediante usuario y contraseña.** |
| **CI** | **Sitio Web** | **SW** | **Productos Computacionales** | **No es necesario.** |
| **IV. Sistema y Sensibilidad de Datos TI** | | | | |
| **Tipo de Datos** | **Clasificaciones de sensibilidad Incluya la calificación para cada índice** | | | |
| | **Confidencialidad** | **Integridad** | **Disponibilidad** | |
| **Correo electrónico de las personas subscritas a los boletines** | **Alto** | **Moderado** | **Bajo** | |
| **Boletín en formato PDF** | **Bajo** | **Alto** | **Alto** | |
| | | | | |

## 4.4 Identificación de fuentes de amenaza

Las fuentes de amenaza se dividen en dos categorías de acuerdo a la publicación especial de la norma NIST 800-30:

• Adversarial

• No adversarial

Las fuentes de amenaza adversariales son producidas por una persona que tiene la intención de realizar un daño o extraer información de manera malintencionada a una empresa. Mientras que las fuentes de amenaza no adversarial son aquellas que se producen sin un grado de intención como errores o desastres naturales.

### 4.4.1 Escala de valoración de fuentes de amenaza

Fuentes de amenazas capaces de iniciar eventos de amenaza.

En la siguiente tabla se indica los valores cualitativos y cuantitativos con los que puede ser calificado un adversario con un nivel de capacidad para ejecutar un ataque informático de diferente tipo.

**Tabla 10 Escala de Evaluación – Características de la Capacidad de Adversario.**

| Valores Cualitativos | Valores Cuantitativos | | Descripción |
|---|---|---|---|
| **Muy Alto** | 96-100 | 10 | El adversario tiene un nivel muy sofisticado de experiencia, está bien dotada de recursos, y puede generar oportunidades para soportar múltiples ataques con éxito, continuos y coordinados. |
| **Alto** | 80-95 | 8 | El adversario tiene un sofisticado nivel de experiencia, recursos y oportunidades significativas para soportar múltiples ataques coordinados con éxito. |

| | | | |
|---|---|---|---|
| **Moderado** | 21-79 | 5 | El adversario tiene recursos moderados, experiencia y oportunidades para soportar múltiples ataques con éxito. |
| **Bajo** | 5-20 | 2 | El adversario tiene recursos limitados, la experiencia y las oportunidades para apoyar un ataque con éxito. |
| **Muy Bajo** | 0-4 | 0 | El adversario tiene muy pocos recursos, conocimientos y oportunidades para apoyar un ataque con éxito. |

En la siguiente tabla se indica los valores cualitativos y cuantitativos con los que puede ser calificado un adversario con un nivel de intención para ejecutar un ataque informático.

**Tabla 11 Evaluación de Escala – Características de Intención del Adversario.**

| Valores Cualitativos | Valores Cuantitativos | | Descripción |
|---|---|---|---|
| **Muy Alto** | 96-100 | 10 | El adversario tiene un nivel muy sofisticado de experiencia, está bien dotada de recursos, y puede generar oportunidades para soportar múltiples ataques con éxito, continuos y coordinados. |
| **Alto** | 80-95 | 8 | El adversario tiene un sofisticado nivel de experiencia, recursos y oportunidades significativas para soportar múltiples ataques coordinados con éxito. |
| **Moderado** | 21-79 | 5 | El adversario tiene recursos moderados, experiencia y oportunidades para soportar múltiples ataques con éxito. |
| **Bajo** | 5-20 | 2 | El adversario tiene recursos limitados, la experiencia y las oportunidades para apoyar un ataque con éxito. |
| **Muy Bajo** | 0-4 | 0 | El adversario tiene muy pocos recursos, conocimientos y oportunidades para apoyar un ataque con éxito. |

En la siguiente tabla se indica los valores cualitativos y cuantitativos con los que puede ser calificado cual es el grado de interés y como escoge a quien atacar el adversario. Los rangos de valor califican si el ataque es específico a una empresa en especial o si se trata de una vulnerabilidad genérica que se puede intentar explotar en cualquier servidor libre.

**Tabla 12 Evaluación de Escala – Características de Orientación del Adversario.**

| Valores Cualitativos | Valores Cuantitativos | | Descripción |
|---|---|---|---|
| **Muy Alto** | 96-100 | 10 | El adversario analiza la información obtenida mediante reconocimiento y ataques para perseguir persistentemente una organización específica, una empresa, un programa, una misión o una función empresarial, centrándose en información, recursos, flujos de suministro o funciones específicos de alto valor o de misión crítica; Empleados o puestos específicos; Proveedores / proveedores de infraestructura de apoyo; O asociaciones. |
| **Alto** | 80-95 | 8 | El adversario analiza la información obtenida a través del reconocimiento para perseguir persistentemente una organización específica, una empresa, un programa, una misión o una función empresarial, centrándose en información, recursos, flujos de suministro o funciones específicos de alto valor o misión, empleados específicos que apoyan esas funciones o posiciones clave. |
| **Moderado** | 21-79 | 5 | El adversario analiza la información disponible públicamente para dirigirse a organizaciones persistentemente específicas de alto valor (y posiciones clave, tales como Director de Información), programas o información. |
| **Bajo** | 5-20 | 2 | El adversario utiliza la información disponible públicamente para dirigirse a una clase de organizaciones o información de alto valor y busca |

| | | | |
|---|---|---|---|
| | | | objetivos de oportunidad dentro de esa clase. |
| **Muy Bajo** | 0-4 | 0 | El adversario puede o no dirigirse a organizaciones o clases específicas de organizaciones. |

En la siguiente tabla se indica los valores cualitativos y cuantitativos con los que puede ser calificado un evento no-adversarial con un nivel negativo de afectación a la empresa si se diera la realización de este evento.

**Tabla 13 Escala de Evaluación – Gama de Efectos para Fuentes de Amenaza No Adversariales.**

| Valores Cualitativos | Valores Cuantitativos | | Descripción |
|---|---|---|---|
| **Muy Alto** | 96-100 | 10 | Los efectos del error, accidente, o acto de la naturaleza están barriendo, implicando casi la totalidad de los recursos cibernéticos del [Nivel 3: sistemas de información; Nivel 2: procesos de misión / negocio o segmentos EA, infraestructura común o servicios de apoyo; Nivel 1: organización / estructura de gobierno]. |
| **Alto** | 80-95 | 8 | Los efectos del error, accidente o acto de la naturaleza son extensos, implicando la mayor parte de los recursos cibernéticos del [Nivel 3: sistemas de información; Nivel 2: procesos de misión / negocio o segmentos EA, infraestructura común o servicios de apoyo; Nivel 1: organización / estructura de gobierno], incluyendo muchos recursos críticos. |
| **Moderado** | 21-79 | 5 | Los efectos del error, accidente o acto de la naturaleza son amplios, implicando una porción significativa de los recursos cibernéticos del [Nivel 3: sistemas de información; Nivel 2: procesos de misión / negocio o segmentos EA, infraestructura común o servicios de apoyo; Nivel 1: organización / estructura |

| | | | |
|---|---|---|---|
| | | | de gobierno], incluyendo algunos recursos críticos. |
| **Bajo** | 5-20 | 2 | Los efectos del error, accidente o acto de la naturaleza son limitados, involucrando algunos de los recursos cibernéticos del [Nivel 3: sistemas de información; Nivel 2: procesos de misión / negocio o segmentos EA, infraestructura común o servicios de apoyo; Nivel 1: organización / estructura de gobierno], pero sin recursos críticos. |
| **Muy Bajo** | 0-4 | 0 | Los efectos del error, accidente o acto de la naturaleza son mínimos, que implican pocos o ninguno de los recursos cibernéticos del [Nivel 3: sistemas de información; Nivel 2: procesos de misión / negocio o segmentos EA, infraestructura común o servicios de apoyo; Nivel 1: organización / estructura de gobierno], y sin recursos críticos. |

### 4.4.2 Valoración de fuentes de amenaza

De acuerdo a las escalas de evaluación de las características de Capacidad, Intención y Orientación del adversario se procedió a la valoración de las fuentes de amenaza.

**Tabla 14 Identificación de Fuentes de Amenaza Adversarial.**

| Id | Fuente de amenaza Fuente de Información | En alcance | Capacidad | Intención | Orientación |
|---|---|---|---|---|---|
| **1** | Adversario-Individuo-intruso | Si | Moderado | Moderado | Bajo |
| **2** | Adversario-individuo - Interno con Privilegios | Si | Muy Alto | Muy Alto | Alto |

De acuerdo a la escala de evaluación de rangos de efectos para fuentes de amenazas no adversariales se procedió a la valoración de las fuentes de amenaza no adversariales.

**Tabla 15 Identificación de Fuentes de Amenaza No – Adversarial.**

| Id | Fuente de amenaza Fuente de Información | En alcance | Rango de efectos |
|---|---|---|---|
| 1 | Accidental usuario | Si | Moderado |
| 2 | Accidental Usuario Privilegiado/Administrador | Si | Muy Alto |
| 3 | Estructural Almacenamiento | Si | Moderado |
| 4 | Estructural Software Network | Si | Alto |
| 5 | Estructural Control de Temperatura y Humedad | Si | Alto |
| 6 | Estructural Fuente de Poder | Si | Alto |
| 7 | Estructural Sistema Operativo | Si | Alto |
| 8 | Ambiente Fuego | Si | Alto |
| 9 | Ambiente Terremoto | Si | Muy Alto |
| 10 | Ambiente Telecomunicaciones | Si | Muy Alto |
| 11 | Ambiente Poder eléctrico | Si | Bajo |
| 12 | Aplicación de propósito general | Si | Alto |

## 4.5 Eventos de amenaza

Acontecimientos de amenaza representantes iniciados por fuentes de amenaza.

Las amenazas estuvieron identificadas por:

Reuniones con miembro del área de sistemas, personal técnico, Administrador de sistema y una comisión de las otras áreas responsables

del buen funcionamiento del centro de investigación para obtener información específica sobre el funcionamiento el sistema.

Revisión de incidentes anteriores de amenazas ocurridos por la explotación de vulnerabilidades en el sistema.

### 4.5.1 Escala de valoración de eventos de amenaza

En la siguiente tabla se indica los valores cuantitativos con los que puede ser calificada la relevancia de un evento de amenaza.

**Tabla 16 Relevancia de los Acontecimientos de Amenaza.**

| Valor | Descripción |
|---|---|
| **Confirmado** | El evento de amenaza o TTP ha sido visto por la organización. |
| **Esperado** | El evento de amenaza o TTP ha sido visto por los compañeros o socios de la organización. |
| **Anticipado** | El evento de amenaza o TTP ha sido reportado por una fuente confiable. |
| **Predicho** | El evento de amenaza o TTP ha sido predicho por una fuente confiable. |
| **Posible** | El evento de amenaza o TTP ha sido descrito por una fuente algo creíble. |
| **N / A** | El evento de amenaza o TTP no es actualmente aplicable. Por ejemplo, un evento de amenaza o TTP podría asumir tecnologías, arquitecturas o procesos específicos que no están presentes en la organización, proceso de misión / negocio, segmento de EA o sistema de información; O condiciones predisponentes que no están presentes (por ejemplo, ubicación en una llanura de inundación). Alternativamente, si la organización utiliza información de amenaza detallada o específica, un evento de amenaza o TTP podría considerarse inaplicable porque la información indica que no se espera que ningún adversario inicie el evento de amenaza o utilice el TTP. |

### 4.5.2 Identificación de eventos de amenaza

De acuerdo a la escala de evaluación de relevancia de los acontecimientos de amenaza se procedió a la valoración de los eventos de amenaza.

**Tabla 17 Identificación de Eventos de Amenaza.**

| ID | Evento de amenaza Fuente de Información | Fuente de amenaza | Relevancia |
|---|---|---|---|
| **1** | Explotación sistemas de información mal configurados o no autorizados expuestos a Internet. | Adversario-Individuo-intruso | Confirmado |
| **2** | Recopilar información mediante el descubrimiento de información de la organización en código abierto. | Adversario-Individuo-intruso | Confirmado |
| **3** | Aprovechar la eliminación insegura o incompleta de datos en entornos con múltiples inquilinos. | Adversario-Individuo-intruso | Confirmado |
| **4** | Realizar ataques utilizando puertos, protocolos y servicios no autorizados. | Adversario-Individuo-intruso | Confirmado |
| **5** | Lleve a cabo un ataque de denegación de servicio (DoS) simple. | Adversario-Individuo-intruso | Confirmado |
| **6** | Conduzca intentos de inicio de sesión de fuerza bruta / ataques de adivinación de contraseña. | Adversario-Individuo-intruso | Confirmado |
| **7** | Causa pérdida de integridad mediante la creación, eliminación y / o modificación de datos en sistemas de información accesibles al público (p. Ej., Degradación de la web). | Adversario-Individuo-intruso | Posible |
| **8** | Causa pérdida de integridad al contaminar o corromper datos críticos. | Adversario-Individuo-intruso | Posible |

| | | | |
|---|---|---|---|
| **9** | Aprovechar el acceso físico del personal autorizado para acceder a las instalaciones de la organización. | Adversario-individuo - Interno con Privilegios | Posible |
| **10** | Explotación de vulnerabilidades en sistemas de información con tiempo programado para la misión organizacional / operaciones de negocio. | Adversario-individuo - Interno con Privilegios | Posible |
| **11** | Comprometer los sistemas de información críticos a través del acceso físico. | Adversario-individuo - Interno con Privilegios | Posible |
| **12** | Realizar ataques de la cadena de suministro dirigidos a explotar hardware, software o firmware crítico. | Adversario-individuo - Interno con Privilegios | Posible |
| **13** | Causa deterioro / destrucción de componentes y funciones del sistema de información críticos. | Adversario-individuo - Interno con Privilegios | Posible |
| **14** | Causa pérdida de integridad inyectando datos falsos pero creíbles en los sistemas de información organizacional. | Adversario-individuo - Interno con Privilegios | Posible |
| **15** | Obtener acceso no autorizado. | Adversario-individuo - Interno con Privilegios | Posible |
| **16** | Obtenga información / datos confidenciales de sistemas de información de acceso público. | Adversario-individuo - Interno con Privilegios | Posible |
| **17** | Configuración incorrecta de privilegios | Accidental usuario | Confirmado |
| **18** | Manipulación incorrecta de información crítica y / o sensible por parte de usuarios autorizados | Accidental Usuario Privilegiado/ Administrador | Confirmado |
| **19** | Error de disco | Estructural Almacenamiento | Confirmado |
| **20** | Error de disco penetrante | Estructural Almacenamiento | Confirmado |

| | | | |
|---|---|---|---|
| **21** | Agotamiento de recursos | Estructural Software Network | Confirmado |
| **22** | Agotamiento de recursos | Estructural Control de Temperatura y Humedad | Confirmado |
| **23** | Terremoto en la instalación primaria | Estructural Control de Temperatura y Humedad | Confirmado |
| **24** | Agotamiento de recursos | Estructural Fuente de Poder | Confirmado |
| **25** | Introducción de vulnerabilidades en productos de software | Estructural Sistema Operativo | Pronosticado |
| **26** | Terremoto en la instalación primaria | Ambiente Terremoto | Confirmado |
| **27** | Terremoto en la instalación primaria | Ambiente Telecomunicaciones | Confirmado |
| **28** | Terremoto en la instalación primaria | Ambiente Poder eléctrico | Confirmado |
| **29** | Terremoto en la instalación primaria | Aplicación de propósito general | Confirmado |

## 4.6 Vulnerabilidades y condiciones de predisposición

Las vulnerabilidades estuvieron identificadas por:

Reuniones con miembro del área de sistemas, personal técnico, Administrador de sistema y una comisión de las otras áreas responsables del buen funcionamiento del centro de investigación para obtener información específica sobre el funcionamiento el sistema.

Revisión de incidentes anteriores de problemas ocurridos por la explotación de vulnerabilidades en el sistema.

### 4.6.1 Escala de valoración vulnerabilidades y condiciones de predisposición

Factores de riesgo que afectan a la probabilidad de explotación de la amenaza exitosa.

En la siguiente tabla se indica los valores cualitativos y cuantitativos con los que puede ser calificada la gravedad de la vulnerabilidad y su nivel de severidad o explotación.

**Tabla 18 Evaluación de Escala – Gravedad de la Vulnerabilidad.**

| Valores Cualitativos | Valores Cuantitativos | | Descripción |
|---|---|---|---|
| **Muy Alto** | 96-100 | 10 | La vulnerabilidad está expuesta y explotable, y su explotación puede resultar en impactos severos. El control de seguridad pertinente u otra remediación no se implementa y no se planea; O no se puede identificar ninguna medida de seguridad para remediar la vulnerabilidad. |
| **Alto** | 80-95 | 8 | La vulnerabilidad es de gran preocupación, basada en la exposición de la vulnerabilidad y facilidad de explotación y / o en la gravedad de los impactos que podrían resultar de su explotación. Se planifica el control de seguridad pertinente u otra remediación, pero no se implementa; Los controles de compensación están en su |

| | | | |
|---|---|---|---|
| | | | lugar y al menos son mínimamente eficaces. |
| **Moderado** | 21-79 | 5 | La vulnerabilidad es de preocupación moderada, basada en la exposición de la vulnerabilidad y facilidad de explotación y / o en la severidad de los impactos que podrían resultar de su explotación.<br>El control de seguridad pertinente u otra remediación se implementa parcialmente y es algo efectivo. |
| **Bajo** | 5-20 | 2 | La vulnerabilidad es de menor importancia, pero se podría mejorar la eficacia de la remediación.<br>El control de seguridad pertinente u otra remediación es completamente implementado y algo efectivo. |
| **Muy Bajo** | 0-4 | 0 | La vulnerabilidad no es motivo de preocupación.<br>El control de seguridad pertinente u otra remediación se implementa, evalúa y es efectivo. |

En la siguiente tabla se indica el tipo de condición predisponente y una descripción de como esto afecta la vulnerabilidad.

**Tabla 19 Taxonomía de las Condiciones de predisposición.**

| Tipo de condición predisponente | Descripción |
|---|---|
| **INFORMACIÓN RELACIONADA**<br>**- Información de seguridad nacional clasificada**<br>**- Compartimientos**<br>**- Información no clasificada controlada**<br>**- Información de identificación personal** | Necesita manejar la información (ya que es creada, transmitida, almacenada, procesada y / o exhibida) de una manera específica, debido a su sensibilidad (o falta de sensibilidad), requisitos legales o reglamentarios y / o acuerdos contractuales u otros acuerdos de organización. |

| | |
|---|---|
| **- Programas especiales de acceso**<br>**- Acuerdo-Determinado NOFORN**<br>**- Propiedad** | |
| **TÉCNICO**<br>**- Arquitectura**<br>**- Cumplimiento de las normas técnicas**<br>**- Uso de productos o líneas de productos específicos**<br>**- Soluciones y / o enfoques para la colaboración basada en el usuario**<br>**Y el intercambio de información**<br>**- Asignación de funciones de seguridad específicas a controles comunes**<br>**- Funcional**<br>**- Multiusuario en red**<br>**- Usuario único**<br>**- Autónomo / no conectado**<br>**- Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados)** | Necesita usar tecnologías de maneras específicas. |
| **OPERACIONAL / AMBIENTAL**<br>**- Movilidad**<br>**- Sitio fijo (especifique la ubicación)**<br>**- Semi-móvil**<br>**- Base terrestre, aeronáutica, marítima, espacial**<br>**- Móvil (por ejemplo, dispositivo de mano)**<br>**- Población con acceso físico y / o lógico a los componentes**<br>**Del sistema de información, misión / proceso de negocio, segmento EA**<br>**- Tamaño de la población**<br>**- Aprobación de la población** | Capacidad para confiar en los controles físicos, de procedimiento y de personal proporcionados por el entorno operacional. |

En la siguiente tabla se indica los valores cualitativos y cuantitativos con los que puede ser calificado la permisividad de las condiciones de predisposición de una vulnerabilidad.

**Tabla 20 Escala de Evaluación – Permisividad de las Condiciones Predisponentes.**

| Valores Cualitativos | Valores Cuantitativos | | Descripción |
|---|---|---|---|
| **Muy Alto** | 96-100 | 10 | Se aplica a todas las misiones organizacionales / funciones empresariales (nivel 1), procesos de misión / negocio (nivel 2) o sistemas de información (nivel 3). |
| **Alto** | 80-95 | 8 | Se aplica a la mayoría de las misiones organizacionales / funciones empresariales (Nivel 1), procesos de misión / negocio (Nivel 2) o sistemas de información (Nivel 3). |
| **Moderado** | 21-79 | 5 | Se aplica a muchas misiones organizacionales / funciones empresariales (nivel 1), procesos de misión / negocio (nivel 2) o sistemas de información (nivel 3). |
| **Bajo** | 5-20 | 2 | Se aplica a algunas misiones organizacionales / funciones empresariales (Nivel 1), procesos de misión / negocio (Nivel 2) o sistemas de información (Nivel 3). |
| **Muy Bajo** | 0-4 | 0 | Se aplica a pocas misiones organizacionales / funciones empresariales (nivel 1), procesos de misión / negocio (nivel 2) o sistemas de información (nivel 3). |

### 4.6.2 Valoración vulnerabilidades y condiciones de predisposición

De acuerdo con la escala de valoración de severidad de la vulnerabilidad se procedió a calificar cada una de las vulnerabilidades encontradas.

**Tabla 21 Identificación de Vulnerabilidades.**

| ID | Vulnerabilidad Fuente de información | Vulnerabilidad Severidad |
|---|---|---|
| **1** | Explotación de servidores en la DMZ de los sistemas de envió masivo | Alto |
| **2** | Recopilación de información de la base de datos de subscriptores del sistema de envío masivo | Bajo |
| **3** | Eliminación de datos en el hosting donde se guarda la información de los boletines. | Moderado |
| **4** | Quedar marcado como servidor de hacking y que no se permita por ejemplo el envío de correos electrónicos | Muy Alto |
| **5** | Denegación de servicio por saturación del enlace | Alto |
| **6** | Claves muy fáciles de descifrar, denegación de servicio | Alto |
| **7** | Ataque de hacking al sitio web del centro | Alto |
| **8** | Corrupción de información en la base de datos del sistema de envío masivo o en el sitio web | Alto |
| **9** | Daño en el sistema operativo del sistema de envío masivo | Muy Alto |
| **10** | Daño en el sistema, en la base de datos o el sistema operativo que deje inoperable el sistema de envío masivo de boletines | Muy Alto |
| **11** | Inoperatividad del servidor del sistema de envío de boletines | Alto |

| | | |
|---|---|---|
| **12** | Daño en el centro de datos que altere el funcionamiento del sistema de envíos masivos | Alto |
| **13** | Borrado del sistema de envío de boletines | Muy Alto |
| **14** | Registro de usuarios falsos en el sistema de envío de boletines | Bajo |
| **15** | Proveer contraseñas a especialistas o técnicos para algún mantenimiento o trabajo especializado | Alto |
| **16** | Obtener base de datos de subscriptores del sistema de envío de boletines | Moderado |
| **17** | Borrado de la información por usuario con privilegios mayores a los que se le debe asignar | Moderado |
| **18** | Borrado de la base de datos, mal colocación de plantilla | Moderado |
| **19** | Saturación del disco duro | Alto |
| **20** | Daño en el disco duro | Muy Alto |
| **21** | Saturación o falta del recurso ancho de banda por malfuncionamiento | Alto |
| **22** | Daño de aire acondicionado | Muy Alto |
| **23** | Variación de voltaje que dañe el aire acondicionado | Alto |
| **24** | Daño en el UPS de contingencia | Alto |
| **25** | Vulnerabilidad del sistema operativo por tener una versión desactualizada del mismo | Moderado |
| **26** | Daño o inaccesibilidad en la instalación por terremoto | Alto |
| **27** | Daño o falta en la instalación de red pública de telecomunicaciones por terremoto | Alto |
| **28** | Falta de suministro por daño en la red eléctrica publica | Moderado |
| **29** | Inaccesible por falta de comunicación por terremoto | Moderado |

De acuerdo a la escala de evaluación de permisividad de las condiciones predisponentes se procedió a la valoración de las condiciones predisponentes.

**Tabla 22 Identificación de las Condiciones Predisponentes.**

| ID | Condiciones predisponentes Fuente de información | Capacidad de penetración de la condición |
|---|---|---|
| **1** | Multiusuario en red | Alto |
| **2** | Información de identificación personal | Bajo |

| | | |
|---|---|---|
| **3** | Multiusuario en red | Alto |
| **4** | Multiusuario en red | Alto |
| **5** | Cumplimiento de las normas técnicas | Muy Alto |
| **6** | Información de identificación personal | Alto |
| **7** | Multiusuario en red | Muy Alto |
| **8** | Multiusuario en red | Muy Bajo |
| **9** | Multiusuario en red | Alto |
| **10** | Usuario único | Muy Alto |
| **11** | Usuario único | Muy Alto |
| **12** | Asignación de funciones de seguridad específicas a controles comunes | Alto |
| **13** | Asignación de funciones de seguridad específicas a controles comunes | Alto |
| **14** | Soluciones y / o enfoques para la colaboración basada en el usuario | Moderado |
| **15** | Información de identificación personal | Alto |
| **16** | Información de identificación personal | Moderado |
| **17** | Multiusuario en red | Moderado |
| **18** | Cumplimiento de las normas técnicas | Moderado |
| **19** | Independiente / no conectado | Alto |
| **20** | Independiente / no conectado | Alto |
| **21** | Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | Alto |
| **22** | Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | Muy Alto |
| **23** | Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | Alto |
| **24** | Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | Alto |
| **25** | Cumplimiento de las normas técnicas | Moderado |
| **26** | Cumplimiento de las normas técnicas | Alto |
| **27** | Cumplimiento de las normas técnicas | Alto |
| **28** | Cumplimiento de las normas técnicas | Alto |
| **29** | Multiusuario en red | Moderado |

## 4.7 Impacto

**Efectos de acontecimientos de amenaza en organizaciones, individuos y la nación**

### 4.7.1 Escala de valoración de los impactos de los eventos de amenaza

En la siguiente tabla se indica los valores cualitativos y cuantitativos con los que puede ser calificado un evento no-adversarial con un nivel negativo de afectación a la empresa si se diera la realización de este evento.

**Tabla 23 Escala de Evaluación – Impacto de los Eventos de Amenaza.**

| Valores Cualitativos | Valores Cuantitativos | | Descripción |
|---|---|---|---|
| **Muy Alto** | 96-100 | 10 | Se podría esperar que el evento de amenaza tenga múltiples efectos adversos severos o catastróficos en las operaciones de la organización, los activos de la organización, los individuos, otras organizaciones o la Nación. |
| **Alto** | 80-95 | 8 | Se podría esperar que el evento de amenaza tenga un efecto adverso grave o catastrófico en las operaciones de la organización, los activos de la organización, los individuos, otras organizaciones o la Nación. Un efecto adverso grave o catastrófico significa que, por ejemplo, el evento de amenaza podría: (i) provocar una grave degradación o pérdida de la |

| | | | |
|---|---|---|---|
| | | | capacidad de la misión en una medida y duración que la organización no pueda llevar a cabo una o más de sus funciones primarias ; (ii) resultar en un daño importante a los activos de la organización; (iii) dar lugar a pérdidas financieras importantes; O (iv) resultar en daño severo o catastrófico a personas que implican pérdida de vidas o lesiones graves que amenazan la vida. |
| **Moderado** | 21-79 | 5 | Se podría esperar que el evento de amenaza tenga un serio efecto adverso en las operaciones de la organización, los activos de la organización, los individuos de otras organizaciones o la Nación. Un efecto adverso grave significa que, por ejemplo, el evento de amenaza podría: (i) provocar una degradación significativa de la capacidad de la misión en la medida y duración que la organización pueda desempeñar sus funciones primarias, pero la efectividad de las funciones se reduce significativamente ; (ii) resultar en un daño significativo a los activos de la organización; (iii) dar lugar a pérdidas financieras significativas; O (iv) resultar en un daño significativo a las personas que no implica pérdida de vidas o lesiones graves que amenacen la vida. |
| **Bajo** | 5-20 | 2 | Se podría esperar que el evento de amenaza tenga un efecto adverso limitado sobre las operaciones de la organización, los activos de la organización, los individuos de otras organizaciones o la Nación. Un efecto adverso limitado significa que, por ejemplo, el evento de amenaza podría: (i) provocar una degradación de la capacidad de |

| | | | |
|---|---|---|---|
| | | | la misión en la medida y en la duración que la organización pueda desempeñar sus funciones primarias, pero la efectividad de las funciones se reduce notablemente; (ii) resultar en un daño menor a los activos de la organización; (iii) dar lugar a pérdidas financieras menores; O (iv) resultar en un daño menor a las personas. |
| **Muy Bajo** | 0-4 | 0 | Se podría esperar que el evento de amenaza tenga un efecto adverso insignificante sobre las operaciones de la organización, los activos de la organización, los individuos de otras organizaciones o la Nación. |

### 4.7.2 Valoración de impactos adversos

**Tabla 24 Plantilla – Identificación de Impactos Adversos.**

| Tipo de Impacto | Impacto Activo afectado | Máximo Impacto |
|---|---|---|
| **DAÑO A LAS OPERACIONES** | No se puede ejecutar la misión/visión del centro | Alto |
| **DAÑO A LOS INDIVIDUOS** | Pérdida de información personalmente identificable. | Moderado |
| **DAÑO A LOS ACTIVOS** | Daño o pérdida de activos de información. | Alto |
| **DAÑO A LAS OPERACIONES** | Daño a la imagen o a la reputación (y por lo tanto a las relaciones de confianza futuras o potenciales). | Alto |
| **DAÑO A LAS OPERACIONES** | Incapacidad para realizar las misiones actuales / funciones de negocios de una manera suficientemente oportuna. | Muy Alto |
| **DAÑO A LOS ACTIVOS** | Daño o pérdida de activos de información. | Moderado |
| **DAÑO A LOS ACTIVOS** | Daño o pérdida de activos de información. | Moderado |
| **DAÑO A LOS ACTIVOS** | Daño o pérdida de activos de información. | Alto |
| **DAÑO A LOS ACTIVOS** | Daños o pérdida de sistemas o redes de información. | Alto |

| | | |
|---|---|---|
| **DAÑO A LOS ACTIVOS** | Daños o pérdida de sistemas o redes de información. | Alto |
| **DAÑO A LOS ACTIVOS** | Daños o pérdida de tecnología o equipo de información. | Muy Alto |
| **DAÑO A LOS ACTIVOS** | Daños o pérdida de tecnología o equipo de información. | Muy Alto |
| **DAÑO A LOS ACTIVOS** | Daños o pérdida de sistemas o redes de información. | Alto |
| **DAÑO A LOS ACTIVOS** | Daño o pérdida de activos de información. | Muy Bajo |
| **DAÑO A LOS ACTIVOS** | Daño o pérdida de activos de información. | Moderado |
| **DAÑO A LOS ACTIVOS** | Daños o pérdida de los activos de información | Moderado |
| **DAÑO A LOS ACTIVOS** | Daños o pérdida de los activos de información | Alto |
| **DAÑO A LOS ACTIVOS** | Daños o pérdidas de tecnología o equipo informático | Alto |
| **DAÑO A LOS ACTIVOS** | Daños o pérdida de sistemas o redes de información | Alto |
| **DAÑO A LOS ACTIVOS** | Daño o pérdida de instalaciones físicas. | Muy Alto |
| **DAÑO A LOS ACTIVOS** | Daño o pérdida de instalaciones físicas. | Alto |
| **DAÑO A LOS ACTIVOS** | Daños o pérdidas de tecnología o equipo informático | Alto |
| **DAÑO A LOS ACTIVOS** | Daños o pérdida de los activos de información. | Alto |
| **DAÑO A LOS ACTIVOS** | Daño o pérdida de instalaciones físicas. | Alto |
| **DAÑO A LOS ACTIVOS** | Daños o pérdida de los activos de información. | Alto |
| **DAÑO A LOS ACTIVOS** | Daño o pérdida de instalaciones físicas. | Muy Alto |
| **DAÑO A LOS ACTIVOS** | Daños o pérdida de sistemas o redes de información | Alto |
| **DAÑO A LOS ACTIVOS** | Daño o pérdida de instalaciones físicas. | Moderado |
| **DAÑO A LOS ACTIVOS** | Daños o pérdida de sistemas o redes de información | Moderado |

## 4.8 Determinación de riesgo

### Evaluación del riesgo para organizaciones, individuos y la nación

### 4.8.1 Escala de valoración de la probabilidad

Determinación de la probabilidad de eventos de amenaza que causan impactos adversos.

**Tabla 25 Escala de Evaluación – Probabiliad de Iniciación del Evento de Amenaza (Adversarial).**

| Valores Cualitativos | Valores Cuantitativos | | Descripción |
|---|---|---|---|
| **Muy Alto** | 96-100 | 10 | Es casi seguro que el adversario inicie el evento de amenaza. |
| **Alto** | 80-95 | 8 | Es muy probable que el adversario inicie el evento de amenaza. |
| **Moderado** | 21-79 | 5 | Es algo probable que el adversario inicie el evento de tratamiento. |
| **Bajo** | 5-20 | 2 | Es improbable que el adversario inicie el evento de amenaza |
| **Muy Bajo** | 0-4 | 0 | Es muy improbable que el adversario inicie el evento de amenaza. |

**Tabla 26 Escala de Evaluación – Probabilidad de Evento de Amenaza Ocurrencia (No Adversarial).**

| Valores Cualitativos | Valores Cuantitativos | | Descripción |
|---|---|---|---|
| **Muy Alto** | 96-100 | 10 | Es casi seguro que ocurrirán errores, accidentes o actos de la naturaleza; O se produce más de 100 veces al año. |
| **Alto** | 80-95 | 8 | Es muy probable que ocurra un error, accidente o acto de la naturaleza; O ocurre entre 10-100 veces al año. |
| **Moderado** | 21-79 | 5 | El error, accidente o acto de la naturaleza es algo probable ocurrir; O ocurre entre 1-10 veces al año. |
| **Bajo** | 5-20 | 2 | No es probable que ocurra un error, accidente o acto de la naturaleza; O se produce |

| | | | |
|---|---|---|---|
| | | | menos de una vez al año, pero más de una vez cada 10 años. |
| **Muy Bajo** | 0-4 | 0 | Es muy poco probable que ocurra un error, accidente o acto de la naturaleza; O ocurre menos de una vez cada 10 años. |

**Tabla 27 Escala de Evaluación – Probabilidad de Acción de Amenaza que Resulta en Impactos Adversos.**

| Valores Cualitativos | Valores Cuantitativos | | Descripción |
|---|---|---|---|
| **Muy Alto** | 96-100 | 10 | Si el evento de amenaza se inicia o se produce, es casi seguro que tiene impactos adversos. |
| **Alto** | 80-95 | 8 | Si el evento de amenaza se inicia o se produce, es muy probable que tenga impactos adversos. |
| **Moderado** | 21-79 | 5 | Si el evento de amenaza se inicia o se produce, es algo probable que tenga impactos adversos. |
| **Bajo** | 5-20 | 2 | Si el evento de amenaza se inicia o se produce, es poco probable que tenga impactos adversos. |
| **Muy Bajo** | 0-4 | 0 | Si el evento de amenaza se inicia o se produce, es muy poco probable que tenga impactos adversos. |

## Tabla G-5: escala de evaluación - probabilidad global

**Tabla 28 Escala de Evaluación – Probabilidad Global.**

| Probabilidad de amenaza Evento Iniciación u ocurrencia | Los eventos de amenaza de probabilidad resultan en impactos adversos | | | | |
|---|---|---|---|---|---|
| | Muy Bajo | Bajo | Moderado | Alto | Muy Alto |

| | | | | | |
|---|---|---|---|---|---|
| **Muy Alto** | Bajo | Moderado | Alto | Muy Alto | Muy Alto |
| **Alto** | Bajo | Moderado | Moderado | Alto | Muy Alto |
| **Moderado** | Bajo | Bajo | Moderado | Moderado | Alto |
| **Bajo** | Muy Bajo | Bajo | Bajo | Moderado | Moderado |
| **Muy Bajo** | Muy Bajo | Muy Bajo | Bajo | Bajo | Bajo |

### 4.8.2 Escala de valoración del nivel de riesgo

**Tabla 29 Escala de Evaluación – Nivel de Riesgo (Combinación de Probabilidad e Impacto).**

| **Probabilidad (Evento de amenaza ocurre y resultados en impacto adverso)** | **Nivel de impacto** | | | | |
|---|---|---|---|---|---|
| | Muy Bajo | Bajo | Moderado | Alto | Muy Alto |
| **Muy Alto** | Muy Bajo | Bajo | Moderado | Alto | Muy Alto |
| **Alto** | Muy Bajo | Bajo | Moderado | Alto | Muy Alto |
| **Moderado** | Muy Bajo | Bajo | Moderado | Moderado | Alto |
| **Bajo** | Muy Bajo | Bajo | Bajo | Bajo | Moderado |
| **Muy Bajo** | Muy Bajo | Muy Bajo | Muy Bajo | Bajo | Bajo |

### 4.8.3 Valoración de riesgo adversarial

Esta sección se la puede revisar en el Anexo A.

### 4.8.4 Valoración de riesgo no – adversarial

Esta sección se la puede revisar en el Anexo A.

# CAPÍTULO 5

## IMPLEMENTACIÓN Y PRUEBAS

En este capítulo se realizará el Análisis de Riesgo luego de haber encontrado las vulnerabilidades y amenazas a las que puede estar expuesto el Centro de Investigación, se lo hará mediante un análisis de tratamiento de riesgo donde se especifique la manera de clasificación del tratamiento de riesgo, así también se especificará los riesgos adversariales y no adversariales que podemos encontrar en base a las normas NIST 800-30, la clasificación de dicho riesgo y la correspondiente identificación de controles de seguridad que puedan ser aplicados en base a los Controles establecidos por la Norma ISO 27001, finalmente procederemos a la elaboración de las políticas de seguridad de la Información que debería ser ejecutadas en el Centro para la Seguridad integral de la información manejada en el Centro.

## 5.1 Análisis de tratamiento de riesgo.

Los riesgos se van a clasificar de la siguiente manera:

- Aceptar. – Este tipo de tratamiento de riesgo es el cual la empresa asume y no se realiza ninguna medida de remediación para minimizarlo o eliminarlo.
- Evitar. – Este tipo de tratamiento de riesgo es en el que la empresa evita realizar el proceso o la actividad relacionado con el riesgo de manera que este no suceda.
- Transferir. – Este tipo de tratamiento de riesgo es en el cual la empresa transfiere el riesgo por medio de aseguramiento de un activo o inmueble.
- Mitigar. – Este tipo de tratamiento de riesgo nos indica que este riesgo puede ser disminuido mediante la implementación de controles y políticas.

De acuerdo a estos tipos de tratamiento de riesgo se realizó una clasificación de los Riesgos de acuerdo a las amenazas y vulnerabilidades de los mismos.

**Tabla 30 Riesgos Adversariales.**

| Evento de amenaza | Fuente de amenaza | Vulnerabilidades y condiciones predisponentes | Riesgo | Opción de Tratamiento de Riesgo |
|---|---|---|---|---|
| **Explotación sistemas de información mal configurados o no autorizados expuestos a Internet.** | Adversario-Individuo-intruso | Explotación de servidores en la DMZ del sistema de envío masivo - Multiusuario en red | Alto | Mitigar |
| **Recopilar información mediante el descubrimiento de información de la organización en código abierto.** | Adversario-Individuo-intruso | Recopilación de información de la base de datos de subscriptores del sistema de envío masivo - Información de identificación personal | Moderado | Aceptar |
| **Aprovechar la eliminación insegura o incompleta de datos en entornos con múltiples inquilinos.** | Adversario-Individuo-intruso | Eliminación de datos en el hosting donde se guarda la información de los boletines. - Multiusuario en red | Moderado | Aceptar |
| **Realizar ataques utilizando puertos, protocolos y servicios no autorizados.** | Adversario-Individuo-intruso | Quedar marcado como servidor de hacking y que no se permita por ejemplo el envió de correos electrónicos - Multiusuario en red | Moderado | Aceptar |
| **Lleve a cabo un ataque de denegación** | Adversario-Individuo-intruso | Denegación de servicio por saturación del enlace - | Muy Alto | Mitigar |

| | | | | |
|---|---|---|---|---|
| **de servicio (DoS) simple.** | | Cumplimiento de las normas técnicas | | |
| **Conduzca intentos de inicio de sesión de fuerza bruta / ataques de adivinación de contraseña.** | Adversario-Individuo-intruso | Claves muy fáciles de descifrar, denegación de servicio - Información de identificación personal | Moderado | Aceptar |
| **Causa pérdida de integridad mediante la creación, eliminación y / o modificación de datos en sistemas de información accesibles al público (p. Ej., Degradación de la web).** | Adversario-Individuo-intruso | Ataque de hacking al sitio web del centro - Multiusuario en red | Moderado | Aceptar |
| **Causa pérdida de integridad al contaminar o corromper datos críticos.** | Adversario-Individuo-intruso | Corrupción de información en la base de datos del sistema de envío masivo o en el sitio web - Multiusuario en red | Moderado | Aceptar |
| **Aprovechar el acceso físico del personal autorizado para acceder a las instalaciones de la organización.** | Adversario-individuo - Interno con Privilegios | Daño en el sistema operativo del sistema de envío masivo - Multiusuario en red | Moderado | Aceptar |
| **Explotación de vulnerabilidades en sistemas de información con tiempo** | Adversario-individuo - Interno con Privilegios | Daño en el sistema, en la base de datos o el sistema operativo que deje inoperable el sistema de envío masivo de boletines - Usuario único | Alto | Mitigar |

| | | | | |
|---|---|---|---|---|
| **programado para la misión organizacional / operaciones de negocio.** | | | | |
| **Comprometer los sistemas de información críticos a través del acceso físico.** | Adversario-individuo - Interno con Privilegios | Inoperatividad del servidor del sistema de envío de boletines - Usuario único | Muy Alto | Mitigar |
| **Realizar ataques de la cadena de suministro dirigidos a explotar hardware, software o firmware crítico.** | Adversario-individuo - Interno con Privilegios | Daño en el centro de datos que altere el funcionamiento del sistema de envíos masivos - Asignación de funciones de seguridad específicas a controles comunes | Alto | Mitigar |
| **Causa deterioro / destrucción de componentes y funciones del sistema de información críticos.** | Adversario-individuo - Interno con Privilegios | Borrado del sistema de envío de boletines - Asignación de funciones de seguridad específicas a controles comunes | Moderado | Aceptar |
| **Causa pérdida de integridad inyectando datos falsos pero creíbles en los sistemas de información organizacional.** | Adversario-individuo - Interno con Privilegios | Registro de usuarios falsos en el sistema de envío de boletines - Soluciones y / o enfoques para la colaboración basada en el usuario | Muy Bajo | Aceptar |
| **Obtener acceso no autorizado.** | Adversario-individuo - Interno con Privilegios | Proveer contraseñas a especialistas o técnicos para algún mantenimiento o trabajo especializado - Información de | Bajo | Aceptar |

| | | | | |
|---|---|---|---|---|
| | | identificación personal | | |
| **Obtenga información / datos confidenciales de sistemas de información de acceso público.** | Adversario-individuo - Interno con Privilegios | Obtener base de datos de subscriptores del sistema de envío de boletines - Información de identificación personal | Moderado | Aceptar |

Se procedió a la realización la tipificación de riesgo para las amenazas no-adversariales.

**Tabla 31 Tratameinto de Riesgo No Adversariales.**

| Evento de amenaza | Fuente de amenaza | Vulnerabilidades y condiciones predisponentes | Riesgo | Opción de Tratamiento de Riesgo |
|---|---|---|---|---|
| **Configuración incorrecta de privilegios** | Accidental usuario | Borrado de la información por usuario con privilegios mayores a los que se le debe asignar - Multiusuario en red | Moderado | Aceptar |
| **Manipulación incorrecta de información crítica y / o sensible por parte de usuarios autorizados** | Accidental Usuario Privilegiado/Administrador | Borrado de la base de datos, mal colocación de plantilla - Cumplimiento de las normas técnicas | Bajo | Aceptar |
| **Error de disco** | Estructural Almacenamiento | Saturación del disco duro - Independiente / no conectado | Muy Alto | Mitigar |
| **Error de disco penetrante** | Estructural Almacenamiento | Daño en el disco duro - Independiente / no conectado | Muy Alto | Mitigar |
| **Agotamiento de recursos** | Estructural Software Network | Saturación o falta del recurso ancho de banda por malfuncionamiento - | Alto | Mitigar |

| | | | | |
|---|---|---|---|---|
| | | Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | | |
| **Agotamiento de recursos** | Estructural Control de Temperatura y Humedad | Daño de aire acondicionado - Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | Alto | Mitigar |
| **Terremoto en la instalación primaria** | Estructural Control de Temperatura y Humedad | Variación de voltaje que dañe el aire acondicionado - Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | Moderado | Aceptar |
| **Agotamiento de recursos** | Estructural Fuente de Poder | Daño en el UPS de contingencia - Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | Moderado | Aceptar |
| **Introducción de vulnerabilidades en productos de software** | Estructural Sistema Operativo | Vulnerabilidad del sistema operativo por tener una versión desactualizada del mismo - Cumplimiento de las normas técnicas | Moderado | Aceptar |
| **Terremoto en la instalación primaria** | Ambiente Terremoto | Daño o inaccesibilidad en la instalación por terremoto - Cumplimiento de las normas técnicas | Muy Alto | Mitigar |
| **Terremoto en la instalación primaria** | Ambiente Telecomunicaciones | Daño o falta en la instalación de red pública de telecomunicaciones por terremoto - Cumplimiento de las normas técnicas | Muy Alto | Mitigar |

| | | | | |
|---|---|---|---|---|
| **Terremoto en la instalación primaria** | Ambiente Poder eléctrico | Falta de suministro por daño en la red eléctrica publica - Cumplimiento de las normas técnicas | Muy Alto | Mitigar |
| **Terremoto en la instalación primaria** | Aplicación de propósito general | Inaccesible por falta de comunicación por terremoto - Multiusuario en red | Muy Alto | Mitigar |

## 5.2 Clasificación del riesgo.

De acuerdo a la clasificación de riesgo y reuniones realizadas en conjunto con el centro de investigación se llegó a la resolución de que los riesgos que serán tratados en este esquema de seguridad serán los siguientes:

**Tabla 32 Identificaión de Amenazas, Fuente de Amenaza y Vulnerabilidades – Nivel de Riesgo y Tratamiento.**

| Evento de amenaza | Fuente de amenaza | Vulnerabilidades y condiciones predisponentes | Riesgo | Opción de Tratamiento de Riesgo |
|---|---|---|---|---|
| **Explotación sistemas de información mal configurados o no autorizados expuestos a Internet.** | Adversario -Individuo- intruso | Explotación de servidores en la DMZ del sistema de envío masivo - Multiusuario en red | Alto | Mitigar |
| **Lleve a cabo un ataque de denegación de servicio (DoS) simple.** | Adversario -Individuo- intruso | Denegación de servicio por saturación del enlace - Cumplimiento de las normas técnicas | Muy Alto | Mitigar |
| **Explotación de vulnerabilidades en sistemas de información con tiempo programado para la misión** | Adversario - individuo - Interno con Privilegios | Daño en el sistema, en la base de datos o el sistema operativo que deje inoperable el sistema de envío | Alto | Mitigar |

| | | | | |
|---|---|---|---|---|
| **organizacional / operaciones de negocio.** | | masivo de boletines - Usuario único | | |
| **Comprometer los sistemas de información críticos a través del acceso físico.** | Adversario - individuo - Interno con Privilegios | Inoperatividad del servidor del sistema de envío de boletines - Usuario único | Muy Alto | Mitigar |
| **Realizar ataques de la cadena de suministro dirigidos a explotar hardware, software o firmware crítico.** | Adversario - individuo - Interno con Privilegios | Daño en el centro de datos que altere el funcionamiento del sistema de envíos masivos - Asignación de funciones de seguridad específicas a controles comunes | Alto | Mitigar |
| **Error de disco** | Estructural Almacena miento | Saturación del disco duro - Independiente / no conectado | Muy Alto | Mitigar |
| **Error de disco penetrante** | Estructural Almacena miento | Daño en el disco duro - Independiente / no conectado | Muy Alto | Mitigar |
| **Agotamiento de recursos** | Estructural Software Network | Saturación o falta del recurso ancho de banda por malfuncionamiento - Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | Alto | Mitigar |
| **Agotamiento de recursos** | Estructural Control de Temperatu ra y Humedad | Daño de aire acondicionado - Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | Alto | Mitigar |
| **Terremoto en la instalación primaria** | Ambiente Terremoto | Daño o inaccesibilidad en la instalación por terremoto - Cumplimiento de las normas técnicas | Muy Alto | Mitigar |

| | | | | |
|---|---|---|---|---|
| **Terremoto en la instalación primaria** | Ambiente Telecomunicaciones | Daño o falta en la instalación de red pública de telecomunicaciones por terremoto - Cumplimiento de las normas técnicas | Muy Alto | Mitigar |
| **Terremoto en la instalación primaria** | Ambiente Poder eléctrico | Falta de suministro por daño en la red eléctrica publica - Cumplimiento de las normas técnicas | Muy Alto | Mitigar |
| **Terremoto en la instalación primaria** | Aplicación de propósito general | Inaccesible por falta de comunicación por terremoto - Multiusuario en red | Muy Alto | Mitigar |

## 5.3 Implementación de políticas de seguridad.

De acuerdo al análisis de riesgo realizado al proceso de envió de boletines por correo masivo. Se ha tomado la responsabilidad de la creación de un documento de políticas generales para la seguridad de la información en el centro. Identificando y Realizando el siguiente conjunto de Políticas, de acuerdo a los diferentes controles de seguridad que se deben aplicar.

**Tabla 33 Identificación de Controles de Seguridad e Implementación de Políticas de Seguridad.**

| Control | Descripción | Política |
|---|---|---|
| **5.1.1 Conjunto de políticas para la seguridad de la información.** | Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes. | Se ha definido el siguiente conjunto de Políticas para la seguridad de la información del CIIFEN, la misma que será debidamente aprobada por la dirección del Centro de Investigación, así como también publicada y comunicada oportunamente a todos los empleados del Centro y sus partes externas que se consideren pertinentes. |

| | | |
|---|---|---|
| **8.1.3 Uso aceptable de los activos.** | Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. | - Todos los activos de información (como archivos físicos o lógicos, sistemas, servicios y equipos) del CIIFEN que se proporcionen a empleados o usuarios estarán bajo su responsabilidad y deben ser usados únicamente para cumplir con los propósitos del negocio.<br>- Se deberá llevar control detallado de los activos de información así como sobre su ubicación física.<br>- La información deberá estar disponible siempre que se necesite y únicamente para los usuarios autorizados a su acceso.<br>- La información deberá ser modificada únicamente por los usuarios autorizados para realizar cambios sobre la misma, lo cual será responsabilidad de los jefes de área los cuáles velarán por sus departamentos.<br>- Únicamente se aceptará información de fuentes confiables, cualquier archivo de procedencia dudosa o desconocida deberá ser rechazado<br>- Se deberá cumplir estrictamente con las políticas de gestión de medios extraíbles, así como las de controles de acceso físico y lógico. |
| **8.3.1 Gestión de soportes extraíbles.** | Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización. | - Ningún empleado podrá llevar fuera de las instalaciones del CIIFEN medios extraíbles (memorias flash, discos duros externos, memorias micro SD, Smart phones, etc.) propiedades del Centro que contenga información confidencial o sensible del mismo.<br>- Será responsabilidad de los usuarios de los medios extraíbles asegurar que los mismos se encuentren siempre libre de virus o cualquier software malicioso, así como resguardarlos en su lugar de almacenamiento. |
| **8.3.2 Eliminación de soportes.** | Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales. | - Cuando un equipo ya no se utilice ya sea por daño, mal estado o antigüedad se deberá proceder de manera formal a notificar su salida definitiva del inventario.<br>- Cuando cualquier dispositivo de almacenamiento (disco duro interno o externo) se deba dar de baja, se deberá asegurar la existencia o creación de una copia de seguridad para tener respaldo de la información. |
| **9.1.1 Política de** | Se debe establecer, documentar y revisar una | - Todos los sistemas deberán ser accedidos únicamente por los usuarios |

| | | |
|---|---|---|
| **control de accesos.** | política de control de acceso<br>con base en los requisitos del negocio y de seguridad de la información. | autorizados, mediante el uso de nombres de usuario y contraseñas.<br>- Se utilizarán métodos de autenticación seguros para el acceso de usuarios remotos<br>- Se deberán usar contraseñas seguras para todos los accesos a los sistemas del Centro.<br>- Se prohíbe el acceso a redes inalámbricas inseguras cuando se trabaje con información sensible o confidencial del Centro.<br>- Se deberá realizar el cambio de contraseñas para los accesos a los diferentes sistemas del Centro al menos dos veces al año.<br>- Cada usuario es responsable del usuario y contraseña que se le asigne para el acceso a cualquier sistema del Centro y deberá mantenerlos de forma confidencial y segura. |
| **11.1.1 Perímetro de seguridad física.** | Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas<br>que contengan información confidencial o critica, e instalaciones de manejo de información. | - Se implementarán mecanismos de control de acceso a las instalaciones y áreas restringidas del Centro de investigación para que únicamente ingrese el personal autorizado para salvaguardar el centro de datos y los diversos equipos de comunicaciones y cómputo.<br>- Se restringe el acceso físico de áreas restringidas tanto a personal interno como externo del Centro para lo cual se llevará un registro que deberá contener el nombre de la persona el motivo la empresa y las fechas y horas de ingreso y salida del área. |
| **11.1.2 Controles físicos de entrada.** | Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. | - El acceso al cuarto de Servidores estará restringido únicamente al responsable del Área de Tecnología y Sistemas o en caso de ausentarse a un delegado y estará controlado por un carnet de identificación.<br>- Para el ingreso de personas externas al Centro se deberá llevar un control mediante la entrega de una tarjeta de visita.<br>- Se deberá implantar un sistema de detección de intrusos para realizar el control del acceso a las instalaciones del Centro en horas no laborables. |
| **11.1.3 Seguridad de oficinas,** | Se debe aplicar seguridad física a oficinas, recintos e instalaciones. | - El ingreso a las oficinas estará limitado a los empleados del centro y será verificado mediante un carnet de identificación. |

| | | |
|---|---|---|
| **despachos y recursos.** | | |
| **11.1.4 Protección contra las amenazas externas y ambientales.** | Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. | - Se deberá contar con extintores contra fuego en el Data Center y oficinas con equipos de cómputo y comunicaciones y realizar periódicamente su mantenimiento.<br>- Quedará prohibido el consumo de bebida y comida en áreas que contengan equipos de computación así como en todos los lugares que contengan documentos físicos.<br>- Quedará prohibido el consumo de bebidas alcohólicas y cigarrillos en cualquier oficina o instalación del Centro. |
| **11.2.1 Emplazamiento y protección de equipos.** | Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entono, y las posibilidades de acceso no autorizado. | - Todos los equipos tecnológicos deberán estar correctamente ubicados en sitios que cuenten con la debida protección contra cualquier tipo de daño así como restringidos para el acceso de personas no autorizadas para su uso. |
| **11.2.4 Mantenimiento de los equipos.** | Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas. | - Para encender los equipos primero deberá verificar que se encuentra con condiciones ambientales adecuadas.<br>- Para apagar los computadores siempre deberá hacerlo mediante la opción de "Apagar" del sistema operativo y esperar hasta que finalice el proceso de forma normal.<br>- Deberá evitarse tocar las pantallas de equipos con los dedos, uñas o cualquier otro objeto que pueda causar rallones u otro tipo d daños.<br>- No deberá colocar ningún tipo de objeto encima de las laptops o computadores de escritorio.<br>- Está prohibido el consumo de comida o bebidas cerca de cualquier equipo de cómputo o documentación física.<br>- Deberá usarse UPS para todos los computadores y servidores, para protección contra fallas o interrupciones de energía eléctrica.<br>- Se deberá realizar mantenimiento preventivo tanto físico como lógico, periódicamente a todos los equipos, por parte del personal del departamento de TI. |

| | | |
|---|---|---|
| **11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.** | Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o rehúso. | - Es responsabilidad de todos los usuarios que todos los dispositivos de almacenamiento secundario sean retirados de forma segura de los diferentes equipos, así como la verificación de la información en caso de que estos deban ser reutilizados.<br>- Queda prohibido a todos los usuarios almacenar o transportar información confidencial del CIIFEN mediante cualquier dispositivo de almacenamiento secundario.<br>- Será obligación de todos los usuarios tomar las debidas medidas de precaución para evitar la contaminación de virus en cualquiera de los equipos mediante medios extraíbles.<br>- Queda prohibido el uso de dispositivos de almacenamiento externo con la finalidad de guardar o dar a conocer información privada de empleados o usuarios del CIIFEN. |
| **12.3.1 Copias de seguridad de la información.** | Se deben hacer copias de respaldo la información, software e imágenes de los sistemas. y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | - Será responsabilidad del jefe de Tecnologías realizar el respaldo periódico (diario) o copias de seguridad de la información, software y sistemas del CIIFEN en medios extraíbles y asegurar el resguardo adecuado de dichas copias.<br>- Todas las copias de seguridad realizadas en medios de almacenamiento extraíbles deberán ser probadas periódicamente (semanalmente) para asegurar su funcionalidad en caso de necesitarse por cualquier motivo.<br>- El jefe de Tecnologías deberá garantizar la confiabilidad de los medios de almacenamiento secundarios para las copias de seguridad comprobando su correcto estado.<br>- Es responsabilidad del jefe de tecnologías almacenar en un lugar seguro el medio de almacenamiento de los respaldos asegurando su integridad tanto física como lógica y su disponibilidad. |
| **12.4.1 Registro y gestión de eventos de actividad.** | | - Los LOGS de registros y eventos deberán estar disponibles en cualquier momento que se necesiten, para lo cual deberá realizarse un respaldo periódico de los mismos.<br>- Los LOGS deberán ser accedidos únicamente por el personal autorizado del área de Tecnologías, y deberán ser almacenados de forma segura. |

| | | |
|---|---|---|
| | | - Todos los respaldos de información que se realicen deberán quedar registrados en los LOGS del servidor. |
| **12.6.1 Gestión de las vulnerabilidades técnicas.** | Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. | - Realización de procedimientos de aseguramiento preventivo de equipos.<br>- Realización de pruebas de penetración sobre los sistemas.<br>- Tener actualizada la base de datos de vulnerabilidades que afecten los activos físicos y lógicos del centro. |
| **12.6.2 Restricciones en la instalación de software.** | Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios. | - El usuario común no debe tener permisos para instalar software en su estación de trabajo.<br>- La clave de superusuario de servidores solo la podrán conocer los miembros del departamento de sistemas con roles orientados a la administración de servidores y el jefe de sistemas.<br>- La clave de superusuario de las estaciones de trabajo solo las podrán conocer miembros del departamento de sistemas con roles orientados al soporte de usuarios y el jefe de sistemas.<br>- Se llevara un listado de aplicaciones instaladas en estaciones de trabajo. |
| **13.1.1 Controles de red.** | Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones. | - Se utilizará un proxy para la navegación en Internet de los funcionarios del centro.<br>- Se establecerán niveles de acceso privilegiados para los departamentos. |
| **14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.** | La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas. | - Usar encriptación de acuerdo a las normas NIST para comunicaciones<br>- Restringir o bloquear el acceso a páginas web externas que se consideren inseguras<br>- Prohibir a los usuarios el descargar información o programas sin considerar los derechos de autor o las respectivas licencias |
| **15.1.1 Política de seguridad de la** | Los requisitos de seguridad de la información para mitigar los riesgos | - Generar documentación (como el registro en una bitácora de acceso) que indique el tipo de ingreso y los accesos concedidos a las empresas proveedoras |

| | | |
|---|---|---|
| **información para suministradores.** | asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar. | de servicios.<br>- Todo proveedor que deba ingresar al Centro con un equipo deberá registrar dicho equipo en la documentación pertinente.<br>- Todos los proveedores del Centro que tengan acceso a la red o al Centro de Datos deberán cumplir algunas prohibiciones correspondientes como son: descargar cualquier tipo de archivo o programa vía Internet o por cualquier otro medio no autorizado por el Centro, la instalación de cualquier software no autorizado por el Centro, compartir o transferir archivos vía internet u cualquier otro medio con fines distintos a los laborales, dañar física o lógicamente los equipos, Reubicar, desconectar, conectar o cambiar la configuración de cualquier equipo sin la autorización correspondiente del departamento de TI del Centro. |
| **15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.** | Se deben establecer y acordar todos los requisitos de seguridad de la información pertinente con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización. | - Establecer una revisión antes, durante y después de la adquisición de equipos de infraestructura de TI.<br>- Asegurar el cumplimiento de las políticas de seguridad con respecto a los suministradores.<br>- Todos los proveedores deberán respetar las reglas y políticas de acceso al Centro de Datos o a la red del Centro cuando requieran acceso a los mismos. |
| **15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.** | Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación. | - Incluir acuerdos de confidencialidad en los contratos con Proveedores, que aseguren que la información proporcionada a los mismos no sea divulgada o compartida por ningún medio, así como tampoco modificada o destruida ya sea de forma intencional o accidental.<br>- Los Proveedores sólo podrán tener acceso a los equipos programas o información con la debida autorización del Jefe del Departamento de TI.<br>- Los Proveedores con acceso al Sistema del Centro no podrá bajo ningún concepto intentar violar las seguridades del mismo. |
| **15.2.1 Supervisión y revisión** | Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación | -Realización de pruebas de rendimiento de los servicios prestados por los proveedores.<br>-Revisión de cumplimiento de métricas. |

| | | |
|---|---|---|
| **de los servicios prestados por terceros.** | de servicios de los proveedores. | -Revisión del acuerdo de servicio (SLA).<br>-Realización de auditoria del área de tecnologías de la información.<br>-Documentación de procedimientos. |
| **15.2.2 Gestión de cambios en los servicios prestados por terceros.** | Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaluación de los riesgos. | -Realización de cambios de accesos en los aplicativos de la empresa manejados por servicios de terceros.<br>-Realización de eliminación de usuarios relacionados con los proveedores anteriores.<br>-Documentación de procedimientos. |
| **16.1.3 Notificación de puntos débiles de la seguridad.** | Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. | -Generación de reporte de vulnerabilidad por parte del ingeniero de seguridad encargado.<br>-Reporte de vulnerabilidad por parte del usuario.<br>-Documentación de procesos de tratamiento de vulnerabilidades de seguridad de la información. |
| **16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.** | Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información. | -Generar una base de conocimiento sobre eventos y vulnerabilidades relacionadas con la seguridad de la información.<br>-Generación de base de datos de vulnerabilidades de seguridad de la información de la empresa.<br>-Realización de un análisis de riesgo tecnológico. |
| **16.1.5 Respuesta a los incidentes** | Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con | -Documentación de procedimiento de gestión de incidentes de seguridad.<br>-Realización de una prueba de penetración contra el software o hardware de la vulnerabilidad identificada causante |

| | | |
|---|---|---|
| **de seguridad.** | procedimientos documentados. | del incidente.<br>-Realización de procedimiento de aseguramiento de servidores antes de la puesta en producción. |
| **17.2.1 Disponibilidad de instalaciones para el procesamiento de la información** | Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. | -Realización de diseños de infraestructura y software que incluyan redundancia a nivel de almacenamiento e infraestructura.<br>-Realización de plan de continuidad de negocios del departamento de tecnologías de información.<br>-Documentación de procedimiento de respaldo de configuración de infraestructura y servicios de tecnologías de la información. |
| **18.1.4 Protección de datos y privacidad de la información personal.** | Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable. | - Documentación de procedimientos de privacidad y protección de datos de acuerdo a la legislación y reglamentos pertinentes.<br>- Incluir acuerdos de confidencialidad en los contratos de empleados internos, consultores y empresas proveedoras, que aseguren que la información proporcionada a los mismos no sea divulgada o compartida por ningún medio, así como tampoco modificada o destruida ya sea de forma intencional o accidental. |

## 5.4 Implementación de controles de seguridad.

Para cada una de las amenazas adversariales y no adversariales se encontró una serie de controles que ayudaran a mitigar el riesgo en el centro de investigación.

**Tabla 34 Implementación de Controles de Seguridad de acuerdo a las Amenazas y Vulnerabilidades.**

| Evento de amenaza | Fuente de amenaza | Vulnerabilidades y condiciones predisponentes | Controles |
|---|---|---|---|
| **Explotación sistemas de información mal configurados o no autorizados expuestos a Internet.** | Adversario-Individuo-intruso | Explotación de servidores en la DMZ del sistema de envío masivo - Multiusuario en red | 12.6.1 Gestión de las vulnerabilidades técnicas. 12.4.1 Registro y gestión de eventos de actividad. 12.3.1 Copias de seguridad de la información. 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. |
| **Lleve a cabo un ataque de denegación de servicio (DoS) simple.** | Adversario-Individuo-intruso | Denegación de servicio por saturación del enlace - Cumplimiento de las normas técnicas | 16.1.3 Notificación de puntos débiles de la seguridad. 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 Respuesta a los incidentes de seguridad. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información |
| **Explotación de vulnerabilidades en sistemas de información con tiempo programado para la misión organizacional / operaciones de negocio.** | Adversario-individuo – Interno con Privilegios | Daño en el sistema, en la base de datos o el sistema operativo que deje inoperable el sistema de envío masivo de boletines - Usuario único | 5.1.1 Conjunto de políticas para la seguridad de la información. 9.1.1 Política de control de accesos. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 16.1.5 Respuesta a los incidentes de seguridad. |
| **Comprometer los sistemas de información críticos a través del** | Adversario-individuo – Interno con Privilegios | Inoperatividad del servidor del sistema de envío de boletines - Usuario único | 11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.2.1 Emplazamiento y |

| | | | |
|---|---|---|---|
| **acceso físico.** | | | protección de equipos.<br>12.3.1 Copias de seguridad de la información. |
| **Realizar ataques de la cadena de suministro dirigidos a explotar hardware, software o firmware crítico.** | Adversario-individuo – Interno con Privilegios | Daño en el centro de datos que altere el funcionamiento del sistema de envíos masivos - Asignación de funciones de seguridad específicas a controles comunes | 15.1.1 Política de seguridad de la información para suministradores.<br>15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.<br>15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.<br>15.2.1 Supervisión y revisión de los servicios prestados por terceros.<br>15.2.2 Gestión de cambios en los servicios prestados por terceros. |
| **Error de disco** | Estructural Almacenamiento | Saturación del disco duro - Independiente / no conectado | 8.3.1 Gestión de soportes extraíbles.<br>8.3.2 Eliminación de soportes.<br>11.2.4 Mantenimiento de los equipos.<br>11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.<br>12.3.1 Copias de seguridad de la información.<br>18.1.4 Protección de datos y privacidad de la información personal. |
| **Error de disco penetrante** | Estructural Almacenamiento | Daño en el disco duro - Independiente / no conectado | 8.3.1 Gestión de soportes extraíbles.<br>8.3.2 Eliminación de soportes.<br>11.1.4 Protección contra las amenazas externas y ambientales.<br>11.2.4 Mantenimiento de los equipos.<br>11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.<br>12.3.1 Copias de seguridad de la información.<br>18.1.4 Protección de datos y privacidad de la información personal. |
| **Agotamiento de recursos** | Estructural Software Network | Saturación o falta del recurso ancho de banda por malfuncionamiento - Funcionalidad | 15.2.1 Supervisión y revisión de los servicios prestados por terceros.<br>15.2.2 Gestión de cambios en los servicios prestados por |

| | | | |
|---|---|---|---|
| | | restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | terceros.<br>13.1.1 Controles de red. |
| **Agotamiento de recursos** | Estructural Control de Temperatura y Humedad | Daño de aire acondicionado - Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | 8.1.3 Uso aceptable de los activos.<br>11.2.4 Mantenimiento de los equipos. |
| **Terremoto en la instalación primaria** | Ambiente Terremoto | Daño o inaccesibilidad en la instalación por terremoto - Cumplimiento de las normas técnicas | 11.1.4 Protección contra las amenazas externas y ambientales. |
| **Terremoto en la instalación primaria** | Ambiente Telecomunicaciones | Daño o falta en la instalación de red pública de telecomunicaciones por terremoto - Cumplimiento de las normas técnicas | 11.1.4 Protección contra las amenazas externas y ambientales. |
| **Terremoto en la instalación primaria** | Ambiente Poder eléctrico | Falta de suministro por daño en la red eléctrica publica - Cumplimiento de las normas técnicas | 11.1.4 Protección contra las amenazas externas y ambientales. |
| **Terremoto en la instalación primaria** | Aplicación de propósito general | Inaccesible por falta de comunicación por terremoto - Multiusuario en red | 11.1.4 Protección contra las amenazas externas y ambientales. |

# CAPÍTULO 6

# ANÁLISIS DE RESULTADOS DEL ESQUEMA DE SEGURIDAD DE UN CENTRO DE INVESTIGACIÓN

## 6.1 Políticas de seguridad propuestas.

### 6.1.1 Resumen

La Dirección de EL CENTRO DE INVESTIGACION, representada en el Comité de Gestión de la Seguridad de la Información, dentro de la estrategia considera la Seguridad de la Información y la de los datos personales como un aspecto vital para garantizar la consecución de los objetivos de negocio. Manteniendo la obligación de garantizar la máxima seguridad de los servicios que se prestan, es decir, la confidencialidad, integridad y disponibilidad de los datos, sistemas y/o comunicaciones gestionadas por EL CENTRO DE INVESTIGACION.

La Dirección de EL CENTRO DE INVESTIGACION se compromete a liderar y fomentar a todos los niveles la seguridad de acuerdo a la Política de Seguridad y los objetivos que en la misma se defina y apruebe, tanto en el ámbito general como en el

particular, y cree un Sistema de Gestión para la Seguridad de la Información (SGSI) que se articule de forma que cumpla los requisitos legales o reglamentarios, gestione la protección y distribución de los activos de la organización, y se encuentre distribuido y publicado en la red corporativa para un mejor conocimiento por parte de todos los empleados.

La presente política se ha elaborado con el consenso del personal incluido en el alcance del Esquema de Seguridad de la Información y ha sido aceptada por el Comité de Gestión de la Seguridad de la Información de EL CENTRO DE INVESTIGACION.

El Comité de Gestión de la Seguridad de la Información de EL CENTRO DE INVESTIGACIÓN se compromete a garantizar la compresión e implicación de todo el personal en el logro de los objetivos del Esquema de Seguridad de la Información.

La presente política será revisada anualmente y se modificará cuando el Comité lo considere pertinente.

### 6.1.2 Introducción

De acuerdo a los riesgos identificados por medio del análisis de riesgo existen muchas falencias en la seguridad lógica del centro de investigación que permiten la filtración de información y la indisponibilidad del servicio. Es por este motivo que la creación de políticas de seguridad de la Información dentro del Centro se considera primordial.

### 6.1.3 Ámbito de aplicación

Las Políticas de Seguridad de la Información que presentamos a continuación se han elaborado de acuerdo al análisis de riesgos y vulnerabilidades realizado en el Centro Internacional para la Investigación del Fenómeno del Niño (CIIFEN), y por lo tanto el ámbito de aplicación de estas políticas se encuentra sujeto a dicho Centro.

### 6.1.4 Objetivos de la política y descripción clara de los elementos involucrados en su definición.

Realización de un esquema de seguridad para el uso de información de manera eficiente de tal manera que el centro pueda realizar sus actividades de manera óptima en el ámbito de las tecnologías de información.

-Resguardar la confidencialidad de la información

-Asegurar la ejecución de los lineamientos establecidos para una correcta utilización de los recursos del centro.

-Asegurar la continuidad de los procesos críticos del centro.

### 6.1.5 Definición.

**Políticas para la gestión de activos**

- Todos los activos de información (como archivos físicos o lógicos, sistemas, servicios y equipos) del CIIFEN que se proporcionen a empleados o usuarios estarán bajo su responsabilidad y deben ser usados únicamente para cumplir con los propósitos del negocio.

- Se deberá llevar control detallado de los activos de información, así como sobre su ubicación física.

- La información deberá estar disponible siempre que se necesite y únicamente para los usuarios autorizados a su acceso.

- La información deberá ser modificada únicamente por los usuarios autorizados para realizar cambios sobre la misma, lo cual será responsabilidad de los jefes de área los cuáles velarán por sus departamentos.

- Únicamente se aceptará información de fuentes confiables, cualquier archivo de procedencia dudosa o desconocida deberá ser rechazado

- Se deberá cumplir estrictamente con las políticas de gestión de medios extraíbles, así como las de controles de acceso físico y lógico.

- Ningún empleado podrá llevar fuera de las instalaciones del CIIFEN medios extraíbles (memorias flash, discos duros externos, memorias micro SD, smartphones, etc.) propiedades del Centro que contenga información confidencial o sensible del mismo.

- Será responsabilidad de los usuarios de los medios extraíbles asegurar que los mismos se encuentren siempre libre de virus o cualquier software malicioso, así como resguardarlos en su lugar de almacenamiento.

- Cuando un equipo ya no se utilice ya sea por daño, mal estado o antigüedad se deberá proceder de manera formal a notificar su salida definitiva del inventario.

- Cuando cualquier dispositivo de almacenamiento (disco duro interno o externo) se deba dar de baja, se deberá asegurar la existencia o creación de una copia de seguridad para tener respaldo de la información.

**Políticas para el control de accesos**

- Todos los sistemas deberán ser accedidos únicamente por los usuarios autorizados, mediante el uso de nombres de usuario y contraseñas.

- Se utilizarán métodos de autenticación seguros para el acceso de usuarios remotos

- Se deberán usar contraseñas seguras para todos los accesos a los sistemas del Centro.

- Se prohíbe el acceso a redes inalámbricas inseguras cuando se trabaje con información sensible o confidencial del Centro.

- Se deberá realizar el cambio de contraseñas para los accesos a los diferentes sistemas del Centro al menos dos veces al año.

- Cada usuario es responsable del usuario y contraseña que se le asigne para el acceso a cualquier sistema del Centro y deberá mantenerlos de forma confidencial y segura.

**Políticas para la seguridad física y ambiental**

- Se implementarán mecanismos de control de acceso a las instalaciones y áreas restringidas del Centro de investigación para que únicamente ingrese el personal autorizado para salvaguardar el centro de datos y los diversos equipos de comunicaciones y cómputo.

- Se restringe el acceso físico de áreas restringidas tanto a personal interno como externo del Centro para lo cual se llevará un registro que deberá contener el nombre de la persona el motivo la empresa y las fechas y horas de ingreso y salida del área.

- El acceso al cuarto de Servidores estará restringido únicamente al responsable del Área de Tecnología y Sistemas o en caso de ausentarse a un delegado y estará controlado por un carnet de identificación.

- Para el ingreso de personas externas al Centro se deberá llevar un control mediante la entrega de una tarjeta de visita.

- Se deberá implantar un sistema de detección de intrusos para realizar el control del acceso a las instalaciones del Centro en horas no laborables.

- El ingreso a las oficinas estará limitado a los empleados del centro y será verificado mediante un carnet de identificación.

- Se deberá contar con extintores contra fuego en el Data Center y oficinas con equipos de cómputo y comunicaciones y realizar periódicamente su mantenimiento.

- Quedará prohibido el consumo de bebida y comida en áreas que contengan equipos de computación, así como en todos los lugares que contengan documentos físicos.

- Quedará prohibido el consumo de bebidas alcohólicas y cigarrillos en cualquier oficina o instalación del Centro.
- Todos los equipos tecnológicos deberán estar correctamente ubicados en sitios que cuenten con la debida protección contra cualquier tipo de daño, así como restringidos para el acceso de personas no autorizadas para su uso.
- Para encender los equipos primero deberá verificar que se encuentra con condiciones ambientales adecuadas.
- Para apagar los computadores siempre deberá hacerlo mediante la opción de "Apagar" del sistema operativo y esperar hasta que finalice el proceso de forma normal.
- Deberá evitarse tocar las pantallas de equipos con los dedos, uñas o cualquier otro objeto que pueda causar rallones u otro tipo d daños.
- No deberá colocar ningún tipo de objeto encima de las laptops o computadores de escritorio.
- Está prohibido el consumo de comida o bebidas cerca de cualquier equipo de cómputo o documentación física.
- Deberá usarse UPS para todos los computadores y servidores, para protección contra fallas o interrupciones de energía eléctrica.

- Se deberá realizar mantenimiento preventivo tanto físico como lógico, periódicamente a todos los equipos, por parte del personal del departamento de TI.

- Es responsabilidad de todos los usuarios que todos los dispositivos de almacenamiento secundario sean retirados de forma segura de los diferentes equipos, así como la verificación de la información en caso de que estos deban ser reutilizados.

- Queda prohibido a todos los usuarios almacenar o transportar información confidencial del CIIFEN mediante cualquier dispositivo de almacenamiento secundario.

- Será obligación de todos los usuarios tomar las debidas medidas de precaución para evitar la contaminación de virus en cualquiera de los equipos mediante medios extraíbles.

- Queda prohibido el uso de dispositivos de almacenamiento externo con la finalidad de guardar o dar a conocer información privada de empleados o usuarios del CIIFEN.

**Políticas para operatividad**

- Será responsabilidad del jefe de Tecnologías realizar el respaldo periódico (diario) o copias de seguridad de la información, software y sistemas del CIIFEN en medios extraíbles y asegurar el resguardo adecuado de dichas copias.

- Todas las copias de seguridad realizadas en medios de almacenamiento extraíbles deberán ser probadas periódicamente (semanalmente) para asegurar su funcionalidad en caso de necesitarse por cualquier motivo.
- El jefe de Tecnologías deberá garantizar la confiabilidad de los medios de almacenamiento secundarios para las copias de seguridad comprobando su correcto estado.
- Es responsabilidad del jefe de tecnologías almacenar en un lugar seguro el medio de almacenamiento de los respaldos asegurando su integridad tanto física como lógica y su disponibilidad.
- Los LOGS de registros y eventos deberán estar disponibles en cualquier momento que se necesiten, para lo cual deberá realizarse un respaldo periódico de los mismos.
- Los LOGS deberán ser accedidos únicamente por el personal autorizado del área de Tecnologías, y deberán ser almacenados de forma segura.
- Todos los respaldos de información que se realicen deberán quedar registrados en los LOGS del servidor.
- Realización de procedimientos de aseguramiento preventivo de equipos.
- Realización de pruebas de penetración sobre los sistemas.

- Tener actualizada la base de datos de vulnerabilidades que afecten los activos físicos y lógicos del centro.

- El usuario común no debe tener permisos para instalar software en su estación de trabajo.

- La clave de supe usuario de servidores solo la podrán conocer los miembros del departamento de sistemas con roles orientados a la administración de servidores y el jefe de sistemas.

- La clave de supe usuario de las estaciones de trabajo solo las podrán conocer miembros del departamento de sistemas con roles orientados al soporte de usuarios y el jefe de sistemas.

- Se llevará un listado de aplicaciones instaladas en estaciones de trabajo.

**Políticas para la seguridad en las telecomunicaciones**

- Se utilizará un proxy para la navegación en Internet de los funcionarios del centro.

- Se establecerán niveles de acceso privilegiados para los departamentos.

**Políticas para la adquisición, desarrollo y mantenimiento de los sistemas de información**

- Usar encriptación de acuerdo a las normas NIST para comunicaciones.

- Restringir o bloquear el acceso a páginas web externas que se consideren inseguras.
- Prohibir a los usuarios el descargar información o programas sin considerar los derechos de autor o las respectivas licencias.

**Políticas para proveedores**

- Generar documentación (como el registro en una bitácora de acceso) que indique el tipo de ingreso y los accesos concedidos a las empresas proveedoras de servicios.
- Todo proveedor que deba ingresar al Centro con un equipo deberá registrar dicho equipo en la documentación pertinente.
- Todos los proveedores del Centro que tengan acceso a la red o al Centro de Datos deberán cumplir algunas prohibiciones correspondientes como son: descargar cualquier tipo de archivo o programa vía Internet o por cualquier otro medio no autorizado por el Centro, la instalación de cualquier software no autorizado por el Centro, compartir o transferir archivos vía internet u cualquier otro medio con fines distintos a los laborales, dañar física o lógicamente los equipos, Reubicar, desconectar, conectar o cambiar la configuración de cualquier equipo sin la autorización correspondiente del departamento de TI del Centro.

- Establecer una revisión antes, durante y después de la adquisición de equipos de infraestructura de TI.
- Asegurar el cumplimiento de las políticas de seguridad con respecto a los suministradores.
- Todos los proveedores deberán respetar las reglas y políticas de acceso al Centro de Datos o a la red del Centro cuando requieran acceso a los mismos.
- Incluir acuerdos de confidencialidad en los contratos con Proveedores, que aseguren que la información proporcionada a los mismos no sea divulgada o compartida por ningún medio, así como tampoco modificada o destruida ya sea de forma intencional o accidental.
- Los Proveedores sólo podrán tener acceso a los equipos programas o información con la debida autorización del Jefe del Departamento de TI.
- Los Proveedores con acceso al Sistema del Centro no podrá bajo ningún concepto intentar violar las seguridades del mismo.
- Realización de pruebas de rendimiento de los servicios prestados por los proveedores.
- Revisión de cumplimiento de métricas.
- Revisión del acuerdo de servicio (SLA).

- Realización de auditoria del área de tecnologías de la información.

- Documentación de procedimientos.

- Realización de cambios de accesos en los aplicativos de la empresa manejados por servicios de terceros.

- Realización de eliminación de usuarios relacionados con los proveedores anteriores.

- Documentación de procedimientos.

**Políticas para gestión de incidentes en la seguridad de la información**

- Generación de reporte de vulnerabilidad por parte del ingeniero de seguridad encargado.

- Reporte de vulnerabilidad por parte del usuario.

- Documentación de procesos de tratamiento de vulnerabilidades de seguridad de la información.

- Generar una base de conocimiento sobre eventos y vulnerabilidades relacionadas con la seguridad de la información.

- Generación de base de datos de vulnerabilidades de seguridad de la información de la empresa.

- Realización de un análisis de riesgo tecnológico.

- Documentación de procedimiento de gestión de incidentes de seguridad.

- Realización de una prueba de penetración contra el software o hardware de la vulnerabilidad identificada causante del incidente.

- Realización de procedimiento de aseguramiento de servidores antes de la puesta en producción.

**Políticas para seguridad de la información en la gestión de la continuidad del negocio**

- Realización de diseños de infraestructura y software que incluyan redundancia a nivel de almacenamiento e infraestructura.

- Realización de plan de continuidad de negocios del departamento de tecnologías de información.

- Documentación de procedimiento de respaldo de configuración de infraestructura y servicios de tecnologías de la información.

**Políticas para cumplimientos legales**

- Documentación de procedimientos de privacidad y protección de datos de acuerdo a la legislación y reglamentos pertinentes.

- Incluir acuerdos de confidencialidad en los contratos de empleados internos, consultores y empresas proveedoras, que

aseguren que la información proporcionada a los mismos no sea divulgada o compartida por ningún medio, así como tampoco modificada o destruida ya sea de forma intencional o accidental.

### 6.1.6 Responsabilidades.

Es responsabilidad del Comité de Seguridad de la Información de Centro la Revisión y control de cumplimiento de las políticas de Seguridad. La responsabilidad de la Difusión y divulgación (por diferentes medios, ya sea de forma verbal por correo electrónico o publicaciones impresas) de las políticas de seguridad a todo el personal está a cargo del Ingeniero de Seguridad.

El cumplimiento fiel de todas las políticas de seguridad de información establecida será responsabilidad de todos los empleados y miembros del Centro de Investigación.

### 6.1.7 Definición de las violaciones

Las políticas de seguridad establecidas deben ser cumplidas y acatadas por todos los empleados y miembros del Centro, las siguientes acciones constituyen violaciones a las mismas y por lo tanto serán sancionadas.

- Incumplimiento de las políticas de seguridad de la información.

- Incumplimiento de las normas y estatutos propios de la empresa.

- Omisión intencional o no intencional de pasos en procedimientos establecidos por el centro.

- Acceso no autorizado a información confidencial o critica del centro.

- Acceso no autorizado a equipos y áreas del departamento de tecnologías de información.

- Uso inapropiado de información confidencial o critica del centro.

- Uso inapropiado de equipos del departamento de tecnologías de información.

### 6.1.8 Sanciones por no cumplir las políticas.

Se han establecido las sanciones a ejecutarse en el caso de incumplimiento de las políticas de seguridad de información, de acuerdo a la Severidad del incumplimiento, definiéndose 3 niveles: Leve, Medio y Alto.

Leve: - Llamado de atención verbal y escrito

Medio: - Envío de Memo.

- Pago de multa por medio de descuento en el rol de pagos.

Alto: - Despido del centro.

- Eliminación de contratos de prestación de servicios.

## 6.2 Controles de seguridad propuestos.

**Tabla 35 Descripción de los Controles de Seguridad.**

| Control | Descripción |
|---|---|
| **5.1.1 Conjunto de políticas para la seguridad de la información.** | Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes. |
| **8.1.3 Uso aceptable de los activos.** | Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. |
| **8.3.1 Gestión de soportes extraíbles.** | Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización. |
| **8.3.2 Eliminación de soportes.** | Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales. |
| **9.1.1 Política de control de accesos.** | Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. |
| **11.1.1 Perímetro de seguridad física.** | Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información. |
| **11.1.2 Controles físicos de entrada.** | Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. |
| **11.1.3 Seguridad de oficinas, despachos y recursos.** | Se debe aplicar seguridad física a oficinas, recintos e instalaciones. |
| **11.1.4 Protección contra las amenazas externas y ambientales.** | Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. |

| | |
|---|---|
| **11.2.1 Emplazamiento y protección de equipos.** | Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado. |
| **11.2.4 Mantenimiento de los equipos.** | Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas. |
| **11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.** | Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó. |
| **12.3.1 Copias de seguridad de la información.** | Se deben hacer copias de respaldo la información, software e imágenes de los sistemas. y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. |
| **12.4.1 Registro y gestión de eventos de actividad.** | |
| **12.6.1 Gestión de las vulnerabilidades técnicas.** | Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición<br>de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. |
| **12.6.2 Restricciones en la instalación de software.** | Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios. |
| **13.1.1 Controles de red.** | Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones. |
| **14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.** | La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas. |
| **15.1.1 Política de seguridad de la información para suministradores.** | Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización<br>se deben acordar con estos y se deben documentar. |
| **15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.** | Se deben establecer y acordar todos los requisitos de seguridad de la información pertinente con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de Tl para la información de la organización. |
| **15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.** | Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación. |

| | |
|---|---|
| **15.2.1 Supervisión y revisión de los servicios prestados por terceros.** | Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores. |
| **15.2.2 Gestión de cambios en los servicios prestados por terceros.** | Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaluación de los riesgos. |
| **16.1.3 Notificación de puntos débiles de la seguridad.** | Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. |
| **16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.** | Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información. |
| **16.1.5 Respuesta a los incidentes de seguridad.** | Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados. |
| **17.2.1 Disponibilidad de instalaciones para el procesamiento de la información** | Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. |
| **18.1.4 Protección de datos y privacidad de la información personal.** | Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable. |

## 6.3 Implementación de un procedimiento de aseguramiento de servidores previo a puesta en producción.

### 6.3.1 Alcance

El procedimiento de aseguramiento de servidores previo a la puesta en producción comprende la planificación e instalación

segura de un servidor. Con esto nos referimos a que en el servidor se encuentra

### 6.3.2 Misión y objetivo del procedimiento

El procedimiento de aseguramiento de servidores previo a puesta en producción tiene como objetivo mitigar los riesgos que se generan cuando se realiza una instalación directa y sin planificación de un servicio o sistema proponiendo un procedimiento que será útil para cualquier servidor nuevo que se quiera instalar en una empresa.

### 6.3.3 Descripción del procedimiento

Las fases para el aseguramiento de un servidor previo a la puesta en producción son dos Planificación e Implementación. Tomar los siguientes pasos para la seguridad del servidor en el contexto de la política de seguridad de la organización debe resultar eficaz:

Planificación

1. Planificar la instalación y la implementación del sistema operativo (SO) y de otros componentes del servidor.

Implementación

2. Instalar, configurar y asegurar el sistema operativo subyacente.

3. Instalar, configurar y asegurar el software del servidor.

**Planificación**

En las etapas de planificación de un servidor, deben considerarse los siguientes elementos:

• Identificar el propósito (s) del servidor.

- ¿Qué categorías de información se almacenarán en el servidor?

- ¿Qué categorías de información serán procesadas o transmitidas a través del servidor?

- ¿Cuáles son los requisitos de seguridad para esta información?

- ¿Se recuperará o almacenará información en otro host (por ejemplo, servidor de bases de datos, servidor de directorios, servidor Web, servidor de almacenamiento conectado a la red (NAS), servidor de red de área de almacenamiento (SAN))?

- ¿Cuáles son los requisitos de seguridad para cualquier otro host involucrado?

- ¿Qué otro (s) servicio (es) será (n) proporcionado (s) por el servidor (en general, dedicar el host a un solo servicio es la opción más segura)?

- ¿Cuáles son los requisitos de seguridad para estos servicios adicionales?

- ¿Cuáles son los requisitos para la continuidad de los servicios prestados por el servidor, como los especificados en la continuidad de los planes de operaciones y planes de recuperación de desastres?

- ¿Dónde estará ubicado el servidor en la red?

• Identificar los servicios de red que se proporcionarán en el servidor, tales como Protocolo de transferencia de hipertexto (HTTP), Protocolo de transferencia de archivos (FTP), Protocolo simple de transferencia de correo (SMTP), Sistema de archivos de red (NFS) o servicios de base de datos (por ejemplo, Open Database Connectivity [ODBC]). También se deben identificar los protocolos de red que se utilizarán para cada servicio (por ejemplo, IPv4, IPv6).

• Identificar cualquier software de servicio de red, tanto de cliente como de servidor, que se instalará en el servidor y en cualquier otro servidor de soporte.

• Identificar los usuarios o categorías de usuarios del servidor y de cualquier host de soporte.

• Determine los privilegios que cada categoría de usuario tendrá en el servidor y en los hosts de soporte.

• Determinar cómo se administrará el servidor (por ejemplo, localmente, remotamente desde la red interna, remotamente desde redes externas).

• Decidir cómo se autenticarán los usuarios y cómo se protegerán los datos de autenticación.

• Determinar cómo se aplicará el acceso adecuado a los recursos de información.

• Determine qué aplicaciones de servidor cumplen con los requisitos de la organización. Considere los servidores que pueden ofrecer una mayor seguridad, aunque con menos funcionalidad en algunos casos. Algunas cuestiones a considerar incluyen:

- Costo
- Compatibilidad con la infraestructura existente
- Conocimiento de los empleados existentes
- Relación de fabricante existente
- Historia de la vulnerabilidad pasada
- Funcionalidad.

• Trabajar en estrecha colaboración con el (los) fabricante (s) en la fase de planificación.

La elección de la aplicación del servidor puede determinar la elección del sistema operativo. Sin embargo, en la medida de

lo posible, los administradores de servidores deben elegir un sistema operativo que proporcione lo siguiente:

- Capacidad para restringir de manera granulada las actividades administrativas o de nivel de root a usuarios autorizados.
- Capacidad de controlar de manera granulada el acceso a los datos en el servidor.
- Posibilidad de deshabilitar los servicios de red innecesarios que pueden incorporarse en el SO o en el software del servidor.
- Capacidad para controlar el acceso a diversas formas de programas ejecutables, como los scripts CGI (Common Gateway Interface) y los complementos de servidor para servidores Web, si es aplicable.
- Capacidad para registrar las actividades apropiadas del servidor para detectar intrusiones e intentos de intrusiones.

Provisión de una capacidad de firewall basada en host para restringir el tráfico entrante y saliente

- Soporte para protocolos de autenticación fuerte y algoritmos de cifrado

Además, las organizaciones deben considerar la disponibilidad de personal capacitado y experimentado para administrar el

servidor. Muchas organizaciones han aprendido la difícil lección de que un administrador capaz y experimentado para un tipo de entorno operativo no es automáticamente tan eficaz para otro.

Muchos servidores alojan información confidencial y muchos otros, como los servidores Web orientados al público, deben ser tratados como sensibles debido al daño a la reputación de la organización que podría ocurrir si la integridad de los servidores se ve comprometida. En estos casos, es fundamental que los servidores están ubicados en entornos físicos seguros. Al planificar la ubicación de un servidor, deben considerarse los siguientes problemas:

¿Están los mecanismos de protección de seguridad física adecuados para el servidor y sus componentes de red (por ejemplo, enrutadores, conmutadores)? Ejemplos incluyen-

- Cerraduras
- Acceso al lector de tarjetas
- Guardias de seguridad
- Sistemas de detección de intrusiones físicas (por ejemplo, sensores de movimiento, cámaras).

¿Hay controles ambientales apropiados para mantener la humedad y la temperatura necesarias? Si se requiere alta disponibilidad, ¿hay controles ambientales redundantes?

¿Existe una fuente de alimentación de respaldo? ¿Por cuánto tiempo proporcionará energía?

¿Hay un equipo adecuado de contención de incendios? ¿Reduce el daño al equipo que de otro modo no sería impactado por el fuego?

Si se requiere alta disponibilidad, ¿hay conexiones de red redundantes? (Para servidores orientados a Internet, generalmente significa conexiones a Internet de al menos dos proveedores de servicios de Internet diferentes.) ¿Existe otro centro de datos que puede ser utilizado para alojar servidores en caso de una catástrofe en el centro de datos original?

Si el lugar está sujeto a desastres naturales conocidos, ¿está endurecido contra esos desastres y / o hay un sitio de contingencia fuera del área potencial del desastre?

Implementación

Para asegurar un servidor se necesita asegurar tanto el sistema operativo como el sistema o servicio que va a operar

en el servidor. Para esto se deberán seguir los siguientes pasos para el aseguramiento del sistema operativo:

Corregir y actualizar el sistema operativo

Eliminar o inhabilitar servicios, aplicaciones y protocolos de red innecesarios

Configure la autenticación del usuario del sistema operativo

Configurar controles de recursos

Instalar y configurar controles de seguridad adicionales, si es necesario

Realizar pruebas de seguridad del sistema operativo.

Para la instalación segura del sistema o servicio se deberán seguir los siguientes pasos:

Instalar o actualizar los programas de soporte básicos del aplicativo en el servidor.

Eliminar o inhabilitar servicios, aplicaciones y contenido de muestra innecesarios.

Configure los controles de acceso y autenticación de usuario del servidor

Configure los controles de recursos del servidor

Pruebe la seguridad de la aplicación de servidor (y el contenido del servidor, si corresponde).

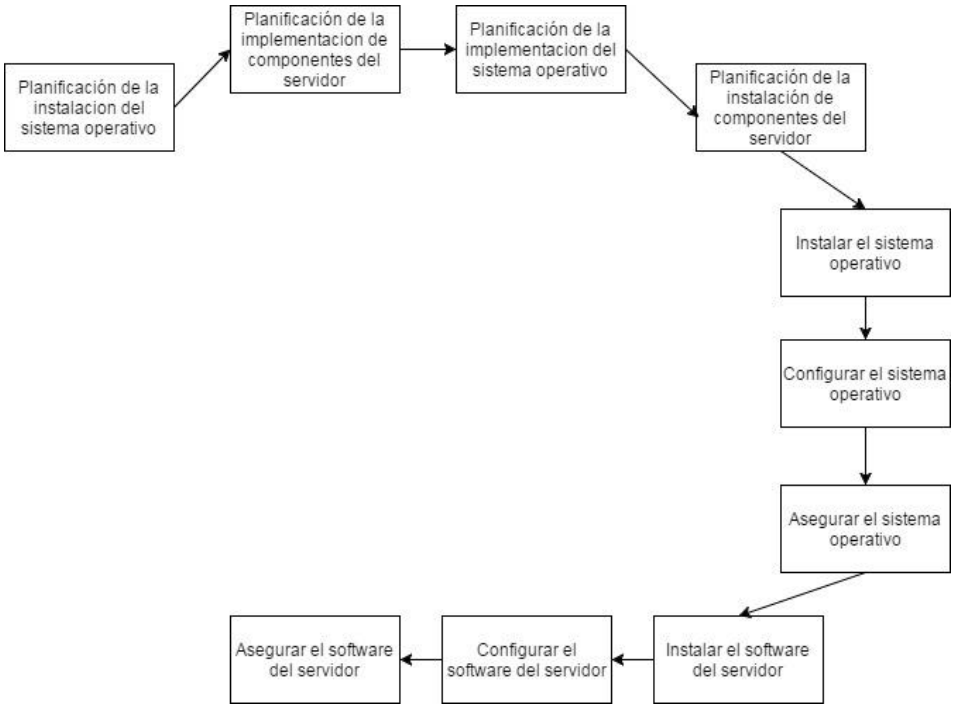


**Figura 6.1 Documentación del Procedimiento de Aseguramiento de un Servidor.**

### 6.3.4 Roles del proceso o responsables del proceso

#### 6.3.4.1 Gerentes de programa de seguridad de sistemas de información

Los Administradores del Programa de Seguridad de Sistemas de Información (ISSPM) supervisan la implementación y el cumplimiento de las normas, reglas y regulaciones especificadas en la política de seguridad de la organización. Los ISSPMs son responsables de las siguientes actividades asociadas a los servidores:

- Asegurar que los procedimientos de seguridad son desarrollados e implementados.
- Asegurar que las políticas de seguridad, las normas y los requisitos se sigan.
- Asegurar que todos los sistemas críticos sean identificados y que existan planes de contingencia, planes de recuperación de desastres y planes de continuidad de operaciones para estos sistemas críticos.
- Asegurar que los sistemas críticos sean identificados y programados para pruebas periódicas de seguridad de acuerdo con los requisitos de política de seguridad de cada sistema respectivo.

#### 6.3.4.2 Oficiales de seguridad de sistemas de información

Los oficiales de seguridad de los sistemas de información (ISSO) son responsables de supervisar todos los aspectos de la seguridad de la información dentro de una entidad organizacional específica. Aseguran que las prácticas de seguridad de la información de la organización cumplan con las políticas, estándares y procedimientos organizacionales y

departamentales. Los ISSOs son responsables de las siguientes actividades asociadas con los servidores:

- Desarrollo de estándares y procedimientos de seguridad internos para los servidores de correo y la infraestructura de red de apoyo
- Cooperar en el desarrollo e implementación de herramientas de seguridad, mecanismos y técnicas de mitigación
- Mantenimiento de los perfiles de configuración estándar de los servidores de correo y la infraestructura de red de soporte controlada por la organización, incluidos, entre otros, sistemas operativos, firewalls, enrutadores y aplicaciones de servidor de correo
- Mantener la integridad operacional de los sistemas mediante la realización de pruebas de seguridad y asegurar que los profesionales de TI designados estén realizando pruebas programadas en sistemas críticos.

#### 6.3.4.3 Administrador de servidor y administradores de red

Los administradores de servidores de correo son arquitectos de sistemas responsables del diseño, implementación y mantenimiento generales de un

servidor de correo. Los administradores de red son responsables del diseño, implementación y mantenimiento generales de una red. Diariamente, el servidor de correo y los administradores de red enfrentan los requisitos de seguridad de los sistemas específicos por los cuales son responsables. Los problemas y soluciones de seguridad pueden originarse desde fuera (por ejemplo, parches de seguridad y arreglos del fabricante o equipos de respuesta a incidentes de seguridad informáticos) o dentro de la organización (por ejemplo, la oficina de seguridad). Los administradores son responsables de las siguientes actividades asociadas con los servidores de correo:

- Instalación y configuración de hosts según las políticas de seguridad de la organización y las configuraciones estándar de sistema / red
- Mantener hosts de forma segura, incluyendo copias de seguridad frecuentes y la aplicación oportuna de parches
- Supervisar la integridad del sistema, los niveles de protección y los eventos relacionados con la seguridad

- Seguimiento de anomalías de seguridad detectadas asociadas a sus recursos de sistema de información
- Realizar pruebas de seguridad según sea necesario.

### 6.3.5 Requerimientos del proceso

El mayor desafío y gasto en el desarrollo y mantenimiento seguro de un servidor es proporcionar los recursos humanos necesarios para realizar adecuadamente las funciones requeridas. Muchas organizaciones no pueden reconocer completamente la cantidad de gastos y las habilidades necesarias para colocar un servidor seguro. Este fracaso a menudo resulta en empleados excesivos y sistemas inseguros. Desde las etapas iniciales de planificación, las organizaciones necesitan determinar las necesidades de recursos humanos necesarias. Los recursos humanos adecuados y suficientes Son el aspecto más importante de la seguridad del servidor. Las organizaciones también deben considerar el hecho de que, en general, las soluciones técnicas no son un sustituto para el personal calificado y experimentado.

Al considerar las implicaciones de recursos humanos de desarrollar y desplegar un servidor, las organizaciones deben considerar lo siguiente:

- Personal requerido- ¿Qué tipo de personal se requiere? Ejemplos de posiciones posibles son administradores de sistemas, administradores de servidores, administradores de red y ISSO.
- Habilidades requeridas- ¿Cuáles son las habilidades necesarias para planificar, desarrollar y mantener adecuadamente el servidor de una manera segura? Algunos ejemplos son la administración del SO, la administración de la red y la programación.
- Personal disponible- ¿Cuáles son los recursos humanos disponibles dentro de la organización? Además, ¿cuáles son sus habilidades actuales y son suficientes para apoyar al servidor? A menudo, una organización descubre que sus recursos humanos existentes no son suficientes y debe considerar las siguientes opciones:
- Capacitar al personal actual-Si el personal está disponible pero no tiene las habilidades requeridas, la organización puede optar por capacitar al personal existente en las habilidades requeridas. Aunque esta es una excelente

opción, la organización debe asegurarse de que los empleados cumplan todos los requisitos previos para la formación.

• Adquirir personal adicional. - Si no hay suficientes miembros del personal disponibles o no tienen las habilidades necesarias, puede ser necesario contratar personal adicional o usar recursos externos.

Una vez que la organización tiene el personal del proyecto y el servidor está activo, será necesario asegurarse de que el número y las habilidades del personal siguen siendo adecuados. Los niveles de amenaza y vulnerabilidad de los sistemas informáticos, incluidos los servidores, están cambiando constantemente, al igual que la tecnología. Esto significa que lo que es adecuado hoy en día puede que no sea mañana, por lo que las necesidades de personal deben ser reevaluadas periódicamente y se llevarán a cabo actividades adicionales de capacitación y otras actividades de capacitación cuando sea necesario.

### 6.3.6 Indicadores del procedimiento

- Cantidad de amenazas y vulnerabilidades encontradas.
- Número de actualizaciones de seguridad instaladas.

- Defectos identificados en el Sistema Operativo o en los Software de Aplicación del Servidor.
- Efectividad del Antivirus y Antispyware Instalados en el Servidor (Cantidad de Virus identificados y eliminados).
- Cantidad de Intentos de Accesos no Autorizados Identificados.
- Cantidad de Monitoreo no Autorizado Identificado.
- Calidad de las Contraseñas utilizadas para el acceso al Software del Servidor.
- Calidad de la Configuración realizada.

# CONCLUSIONES Y RECOMENDACIONES

## Conclusiones

**1.** Se logró identificar las amenazas y vulnerabilidades a las que está expuesto el Centro de Investigación, y a la vez a partir de esto se realizó el correspondiente análisis de riesgo, que permite mitigar y controlar dichas amenazas y vulnerabilidades de forma efectiva, otorgando una mayor seguridad de los Sistemas e información manejada por el Centro, para lo cual fue de suma importancia conocer y utilizar las normativas presentes en tanto en las publicaciones de la NIST en sus series 800 así como de las normas ISO 27001.

**2.** La seguridad de la Información es de vital importancia y trascendencia para toda organización y por ende la implementación de un Sistema de Seguridad se vuelve imprescindible para poder otorgarla. Fue por este motivo que se identificaron los controles de seguridad que deberían ser puestos en práctica por el Centro para poder brindar una adecuada

seguridad a la información y de forma especial al Sistema de Envío de Boletines que es el que utiliza el proceso clave del Centro. Cabe mencionar que estos controles han podido ser identificados basándonos en los correspondientes implementados por la Norma ISO/IEC 27002:2013.

**3.** Un Servidor de es uno de los activos físicos de mayor importancia para un Centro de Investigación, fue por este motivo que se realizó el procedimiento que se debería seguir para Asegurar de forma Integral un Servidor previo su puesta en Producción, además porque uno de los principales motivos para la implementación de un sistema de seguridad es justamente la protección de los activos de la organización mediante la disminución de los riesgos a los cuales pueden estar expuestos. Para explicar dicho procedimiento de aseguramiento ha sido de gran ayuda e importancia conocer la Norma NIST 800-44, la misma que nos brinda todas las directrices que deben seguir cualquier empresa en para asegurar un activo tan importante, como en este caso lo es el Servidor del Sistema de Envío de Boletines del Centro.

**4.** Cómo el esquema de seguridad mitiga riesgos en los procesos críticos de la empresa, otros procesos que no se analizaron esta vez, son candidatos para un futuro análisis de riesgo, procedimientos que se podrían implementar posteriormente. Ya que la gestión de la seguridad

de la información es algo que se debe realizar constantemente en la empresa, y que debe ser llevada a cabo mediante procedimientos sistemáticos que sean debidamente documentados y dados a conocer a todos los miembros de la organización. Así también no se debería implementar los sistemas de seguridad únicamente para controlar amenazas al momento que se presentan, sino más bien de forma anticipada a los hechos en especial sobre los procesos y activos más críticos.

## Recomendaciones

**1.** Se recomienda ampliar y realizar un nuevo análisis de riesgo a futuro para los otros procesos que también se podrían considerar críticos a más del proceso central. También se debería poner en práctica el procedimiento para aseguramiento de servidores previo a su puesta en producción en el centro de investigación, para que se pueda proveer de una adecuada seguridad de este activo tan valioso y de la información manejada por el mismo.

**2.** Se recomienda también que se lleve a la práctica todos los controles y políticas de seguridad realizados en el presente trabajo, para que pueda proveerse de una mayor seguridad al Sistema de Envío de Boletines y a la información del Centro. Ya que las políticas de Seguridad no solo son directrices sino también nos ayudan a mitigar y controlar posibles

amenazas a las que pueden estar expuestos los diferentes activos de información dentro del Centro.

**3.** Finalmente se recomienda se mantenga operando y actualizando constantemente el sistema de seguridad de información del Centro. Puesto que esto les da la ventaja de contar con una metodología empleada internacionalmente por la mayoría de empresas a nivel mundial, ya que se basa en el uso de las Normas ISO 27001 y las Normas NIST, las cuales son herramientas muy valiosas que no solo le dan la seguridad de la información sino a la vez permiten satisfacer de mejor manera las demandas de los usuarios y clientes, al saberse protegidos.

# BIBLIOGRAFÍA

[1] Universidad de Vigo, Área de Ciencias de la Computación e Inteligencia Artificial, http://ccia.ei.uvigo.es/docencia/SSI/normas-leyes.pdf, fecha de consulta mayo 2016

[2] ISO 27000.ES, ISO 27000.ES, http://www.iso27000.es/sgsi.html, fecha de consulta octubre 2016

[3] Advisera, 27001 Academy, http://advisera.com/27001academy/es/que-es-iso-27001, fecha de consulta octubre 2016

[4] ISO Tools, ISO Tools Excellence, https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001, fecha de consulta agosto 2016

[5] National Institute of Standars and Technology, NIST Page, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf, fecha de consulta enero 2017

[6] National Institute of Standars and Technology, NIST Publications, http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf, fecha de consulta enero 2017

[7] National Institute of Standars and Technology, NIST Publications, http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf, fecha de consulta enero 2017

[8] International Organitation for Standardization: ISO 27001 - information security management, ISO/IEC 27001 - Information security management, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm. fecha de consulta mayo 2016.

# Anexo A

## 1 Tablas de Valoración de riesgo adversarial

**Tabla 36 Riesgo Adversarial.**

| Evento de amenaza | Fuente de amenaza | Características de las fuentes de amenaza | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Capacidad | Intención | Orientación | Relevancia | Probabilidad de Iniciación de Ataque | Vulnerabilidades y condiciones predisponentes | Severidad y Penetración | Probabilidad de éxito del ataque iniciado | Probabilidad general | Nivel de Impacto | Riesgo |
| **Explotación sistemas de información mal configurados o no autorizados expuestos a Internet.** | Adversario-Individuo-intruso | Moderado | Moderado | Bajo | Confirmado | Moderado | Explotación de servidores en la DMZ del sistema de envío masivo - Multiusuario en red | Alto | Muy Alto | Alto | Alto | Alto |
| **Recopilar información mediante el descubrimiento de información de la organización en código abierto.** | Adversario-Individuo-intruso | Moderado | Moderado | Bajo | Confirmado | Moderado | Recopilación de información de la base de datos de subscriptores del sistema de envío masivo - | Bajo | Moderado | Moderado | Moderado | Moderado |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Información de identificación personal | | | | | |
| **Aprovechar la eliminación insegura o incompleta de datos en entornos con múltiples inquilinos.** | Adversario-Individuo-intruso | Moderado | Moderado | Bajo | Confirmado | Moderado | Eliminación de datos en el hosting donde se guarda la información de los boletines. - Multiusuario en red | Moderado | Moderado | Moderado | Alto | Moderado |
| **Realizar ataques utilizando puertos, protocolos y servicios no autorizados.** | Adversario-Individuo-intruso | Moderado | Moderado | Bajo | Confirmado | Moderado | Quedar marcado como servidor de hacking y que no se permita por ejemplo el envío de correos electrónicos - Multiusuario en red | Muy Alto | Alto | Moderado | Alto | Moderado |
| **Lleve a cabo un ataque de denegación** | Adversario- | Moderado | Moderado | Bajo | Confirmado | Alto | Denegación de servicio por | Alto | Alto | Alto | Muy Alto | Muy Alto |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **de servicio (DoS) simple.** | Individuo -intruso | | | | | | saturación del enlace - Cumplimiento de las normas técnicas | | | | | |
| **Conduzca intentos de inicio de sesión de fuerza bruta / ataques de adivinación de contraseña.** | Adversario- Individuo -intruso | Moderado | Moderado | Bajo | Confirmado | Moderado | Claves muy fáciles de descifrar, denegación de servicio - Información de identificación personal | Alto | Muy Alto | Alto | Muy Alto | Moderado |
| **Causa pérdida de integridad mediante la creación, eliminación y / o modificación de datos en sistemas de información accesibles al público (p. Ej., Degradación de la web).** | Adversario- Individuo -intruso | Moderado | Moderado | Bajo | Posible | Alto | Ataque de hacking al sitio web del centro - Multiusuario en red | Alto | Alto | Alto | Moderado | Moderado |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Causa pérdida de integridad al contaminar o corromper datos críticos.** | Adversario-Individuo-intruso | Moderado | Moderado | Bajo | Posible | Moderado | Corrupción de información en la base de datos del sistema de envío masivo o en el sitio web - Multiusuario en red | Alto | Moderado | Moderado | Alto | Moderado |
| **Aprovechar el acceso físico del personal autorizado para acceder a las instalaciones de la organización.** | Adversario-individuo - Interno con Privilegios | Muy Alto | Muy Alto | Alto | Posible | Moderado | Daño en el sistema operativo del sistema de envío masivo - Multiusuario en red | Muy Alto | Alto | Moderado | Alto | Moderado |
| **Explotación de vulnerabilidades en sistemas de información con tiempo programado para la misión** | Adversario-individuo - Interno con Privilegios | Muy Alto | Muy Alto | Alto | Posible | Muy Alto | Daño en el sistema, en la base de datos o el sistema operativo que deje inoperable el sistema de envió | Muy Alto | Muy Alto | Muy Alto | Alto | Alto |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **organizacional / operaciones de negocio.** | | | | | | | masivo de boletines - Usuario único | | | | | |
| **Comprometer los sistemas de información críticos a través del acceso físico.** | Adversario-individuo - Interno con Privilegios | Muy Alto | Muy Alto | Alto | Posible | Muy Alto | Inoperatividad del servidor del sistema de envío de boletines - Usuario único | Alto | Muy Alto | Muy Alto | Muy Alto | Muy Alto |
| **Realizar ataques de la cadena de suministro dirigidos a explotar hardware, software o firmware crítico.** | Adversario-individuo - Interno con Privilegios | Muy Alto | Muy Alto | Alto | Posible | Moderado | Daño en el centro de datos que altere el funcionamiento del sistema de envíos masivos - Asignación de funciones de seguridad específicas a controles comunes | Alto | Moderado | Moderado | Muy Alto | Alto |
| **Causa deterioro /** | Adversario- | Muy Alto | Muy Alto | Alto | Posible | Bajo | Borrado del sistema de | Muy Alto | Muy Alto | Moderado | Alto | Moderado |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **destrucción de componentes y funciones del sistema de información críticos.** | individuo - Interno con Privilegios | | | | | | envío de boletines - Asignación de funciones de seguridad específicas a controles comunes | | | | | |
| **Causa pérdida de integridad inyectando datos falsos pero creíbles en los sistemas de información organizacional.** | Adversario-individuo - Interno con Privilegios | Muy Alto | Muy Alto | Alto | Posible | Muy Bajo | Registro de usuarios falsos en el sistema de envío de boletines - Soluciones y / o enfoques para la colaboración basada en el usuario | Bajo | Muy Bajo | Muy Bajo | Muy Bajo | Muy Bajo |
| **Obtener acceso no autorizado.** | Adversario-individuo - Interno con Privilegios | Muy Alto | Muy Alto | Alto | Posible | Muy Bajo | Proveer contraseñas a especialistas o técnicos para algún mantenimiento o trabajo | Alto | Muy Alto | Bajo | Moderado | Bajo |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | especializado - Información de identificación personal | | | | | |
| **Obtenga información / datos confidenciales de sistemas de información de acceso público.** | Adversario-individuo - Interno con Privilegios | Muy Alto | Muy Alto | Alto | Posible | Muy Alto | Obtener base de datos de subscriptores del sistema de envío de boletines - Información de identificación personal | Moderado | Muy Alto | Muy Alto | Moderado | Moderado |

## 2 Tabla de Valoración de riesgo no – adversarial

### Tabla 37 Riesgo No Adversarial.

| Evento de amenaza | Fuente de amenaza | Rango de efectos | Relevancia | Probabilidad de Evento Ocurrido | Vulnerabilidades y condiciones predisponentes | Severidad y Penetración | Probabilidad de los resultados del evento en el impacto adverso | Probabilidad general | Nivel de Impacto | Riesgo |
|---|---|---|---|---|---|---|---|---|---|---|
| **Configuración incorrecta de privilegios** | Accidental usuario | Moderado | Confirmado | Muy Alto | Borrado de la información por usuario con privilegios mayores a los que se le debe asignar - Multiusuario en red | Moderado | Moderado | Moderado | Alto | Moderado |
| **Manipulación incorrecta de información crítica y / o sensible por parte de usuarios autorizados** | Accidental Usuario Privilegiado/ Administrador | Muy Alto | Confirmado | Moderado | Borrado de la base de datos, mal colocación de plantilla - Cumplimiento de las normas técnicas | Moderado | Moderado | Moderado | Alto | Bajo |
| **Error de disco** | Estructural Almacenamiento | Moderado | Confirmado | Muy Alto | Saturación del disco duro - Independiente / no conectado | Alto | Moderado | Moderado | Alto | Muy Alto |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Error de disco penetrante** | Estructural Almacenamiento | Moderado | Confirmado | Alto | Daño en el disco duro - Independiente / no conectado | Muy Alto | Moderado | Moderado | Muy Alto | Muy Alto |
| **Agotamiento de recursos** | Estructural Software Network | Alto | Confirmado | Muy Alto | Saturación o falta del recurso ancho de banda por malfuncionamiento - Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | Alto | Moderado | Moderado | Alto | Alto |
| **Agotamiento de recursos** | Estructural Control de Temperatura y Humedad | Alto | Confirmado | Alto | Daño de aire acondicionado - Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | Muy Alto | Moderado | Moderado | Alto | Alto |
| **Terremoto en la instalación primaria** | Estructural Control de Temperatura y Humedad | Alto | Confirmado | Muy Alto | Variación de voltaje que dañe el aire acondicionado - Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | Alto | Moderado | Moderado | Alto | Moderado |
| **Agotamiento de recursos** | Estructural Fuente de Poder | Alto | Confirmado | Alto | Daño en el UPS de contingencia - Funcionalidad restringida (por ejemplo, comunicaciones, sensores, Controladores integrados) | Alto | Moderado | Moderado | Alto | Moderado |
| **Introducción de vulnerabilidades en productos de software** | Estructural Sistema Operativo | Alto | Pronosticado | Alto | Vulnerabilidad del sistema operativo por tener una versión desactualizada del mismo - Cumplimiento de las normas técnicas | Moderado | Moderado | Muy bajo | Alto | Moderado |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Terremoto en la instalación primaria** | Ambiente Terremoto | Muy Alto | Confirmado | Muy Alto | Daño o inaccesibilidad en la instalación por terremoto - Cumplimiento de las normas técnicas | Alto | Muy Bajo | Moderado | Muy Alto | Muy Alto |
| **Terremoto en la instalación primaria** | Ambiente Telecomunicaciones | Muy Alto | Confirmado | Muy Alto | Daño o falta en la instalación de red pública de telecomunicaciones por terremoto - Cumplimiento de las normas técnicas | Alto | Moderado | Moderado | Alto | Muy Alto |
| **Terremoto en la instalación primaria** | Ambiente Poder eléctrico | Bajo | Confirmado | Muy Alto | Falta de suministro por daño en la red eléctrica publica - Cumplimiento de las normas técnicas | Moderado | Moderado | Bajo | Moderado | Muy Alto |
| **Terremoto en la instalación primaria** | Aplicación de propósito general | Alto | Confirmado | Alto | Inaccesible por falta de comunicación por terremoto - Multiusuario en red | Moderado | Bajo | Moderado | Moderado | Muy Alto |