DISEÑAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA NORMA ISO 27001 EN EL INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR CENTRO ZONAL VIRGEN Y TURÍSTICO DE LA REGIONAL BOLÍVAR

SHIRLEY SANDRA BUENO BUSTOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CARTAGENA
2015

DISEÑAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA NORMA ISO 27001 EN EL INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR CENTRO ZONAL VIRGEN Y TURÍSTICO DE LA REGIONAL BOLIVAR

SHIRLEY SANDRA BUENO BUSTOS

Proyecto de grado requisito para optar el título de ESPECIALISTA EN SEGURIDAD INFORMATICA

Asesor: SALOMON GONZALEZ GARCIA.
Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CARTAGENA
2015

NOTA DE ACEPTACION

_____
_____
_____
_____

_____
Firma del Jurado 1

_____
Firma del Jurado 2

Cartagena Día: ____Mes____Año:2015

DEDICATORIA

Ofrezco este triunfo a mi padre Dios por darme sabiduría y fuerzas para seguir adelante en esta etapa más en mi camino.

A mi madre que me dio la vida, por su amor incondicional, apoyo constante y formación necesaria para realizar mis metas.

A mis hermanas y amigos por demostrarme su respaldo y apoyo.

Shirley Sandra Bueno Bustos.

AGRADECIMIENTO

Doy gracias a mi Dios todopoderoso el cual me ha dado sabiduría, los recursos necesarios y salud para llevar a cabo este proyecto.

A mi madre la cual con su apoyo incondicional, ayudándome en todos las decisiones.

A mi Asesor Salomón Gonzales por brindarme su apoyo incondicional y su buena asesoría durante el desarrollo del proyecto.

A mis docentes por brindarme la oportunidad de adquirir conocimientos y experiencias que contribuyen a mi crecimiento personal y profesional.

A mis amigos y compañeros de vida por animarme a seguir adelante con este proyecto.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXO

Pág.

RESUMEN

El ICBF Centro Zonal Virgen y Turístico Regional Bolívar ubicado en la Ciudad de Cartagena, no cuenta con suficiente normas de seguridad que ayuden a proteger los activos de información, esto ha originado que se presentan diferentes incidentes de seguridad tales como: la perdida de información, daño de equipos informáticos, borrado y modificación de información sensible, infiltración o acceso no autorizado en los sistemas, suplantación de personal, Craqueo de contraseñas, deterioro de activos físicos y dificultad en el acceso a los servicios por parte de terceros, entre otras.

Como respuesta a esta problemática se elabora el presente proyecto, el cual busca diseñar un sistema de gestión de seguridad de la información que permita conocer las vulnerabilidades, amenazas y riesgos a los cuales están expuestos los activos, para así establecer objetivos, políticas, procedimientos y acciones encaminadas a garantizar la confidencialidad, disponibilidad e integridad de los activos de información que tiene la empresa, y de igual forma mantener el nivel de riesgo en un nivel aceptable.

Palabras Claves:
ISO 27001, SGSI, Vulnerabilidad, Activos de Información, MAGERIT, Gestión de Riesgo, Políticas de seguridad.

INTRODUCCIÓN

Los delitos informáticos, el sabotaje, la suplantación, los daños informáticos, la pérdida de información, entre otros, están interrumpiendo las operaciones normales al interior de una organización, lo cual ha obligado a las empresas adoptar medidas y controles de seguridad que permitan garantizar la continuidad del negocio. El ICBF Centro Zonal Virgen y Turístico, no es ajeno a esta problemática, teniendo que afrontar múltiples incidentes de seguridad entre los cuales se mencionan la fuga o perdida de información sensible, perdida de integridad de información digital, infiltración o acceso no autorizado en los sistemas, propagación de virus y software malicioso, suplantación de personal, acceso no autorizado en el sistema de información, deterioro de activos, perdida de documentos, fallas, entre otros.

El presente proyecto busca diseñar un sistema de gestión de seguridad de la información usando la norma ISO 27001:2013 y la metodología MAGERIT para la gestión del riesgo en los activos de información presentes en el ICBF Centro Zonal Virgen y Turístico, Regional Bolívar, garantizando de esta manera la seguridad de la información y un nivel aceptable de riesgo.

1. PLANTEAMIENTO DEL PROBLEMA

Los problemas de seguridad en las empresas son originados por la explotación de vulnerabilidades en los activos de información, ausencia de controles y procedimientos mal definidos. En el ICBF Centro Zonal Virgen y Turístico, existen aamenazas que diariamente afectan a los activos, entre las más destacables podemos mencionar: La pérdida de integridad de información digital, infiltración o acceso no autorizado en los sistemas, propagación de virus y software malicioso, suplantación de personal, uso de contraseñas débiles, deterioro de activos físicos, perdida de documentos, fallas de hardware, problemas de recuperación de información, perdida de documentos físicos, fallas en el Hardware, problemas de recuperación de información, problemas de denegación de servicios, problemas con ubicación en áreas susceptibles a desastres, divulgación de información, información oculta en las memorias USB, equipos dañados, entre otros.

Como alternativa de solución a las problemáticas antes mencionadas, la organización ha planteado la necesidad de diseñar un SGSI, lo cual ha dado origen al siguiente interrogante de investigación ¿cómo Diseñar un Sistema de Gestión de Seguridad de la Información que le permita a la organización Gestionar los riesgos, eliminar las amenazas y dar continuidad al negocio?."

2. JUSTIFICACIÓN.

La información es uno de los activos más valiosos que posee la empresa, debido a su importancia se requiere establecer un conjunto de medidas que permitan la gestión de los riesgos, la preservación de los activos y la continuidad del negocio.

En el ICBF se maneja mucha información de tipo misional entre la que se destaca: Primera Infancia, Sistema nacional de bienestar familiar, Programa de adopciones, Familias con Bienestar, Responsabilidad Penal, Nutrición, Desayuno infantil con amor, entre otros, igualmente se maneja información confidencial sobre los clientes (niños beneficiados), proveedores y diversos entes gubernamentales. Debido al nivel de confidencialidad que requieren los datos se hace necesario plantear un conjunto de medidas para mitigar problemas de seguridad al interior de la institución.

El desarrollo del presente proyecto busca satisfacer la necesidad de seguridad presente en la institución antes mencionada, garantizando la confidencialidad, disponibilidad e integridad de los datos, e igualmente procurando un nivel de riesgo aceptable para la organización, apoyados siempre en el diseño de un Sistema de gestión de seguridad de la información.

.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información utilizando la norma ISO 27001:2013 en el ICBF Centro Zonal Virgen y Turístico, Regional Bolívar.

3.2 OBJETIVOS ESPECIFICOS

Identificar las vulnerabilidades que afectan los activos del ICBF centro zonal Virgen y Turístico Regional Bolívar.

Identificar las amenazas de seguridad informática que afectan los activos de la organización mediante un análisis de vulnerabilidades.

Establecer los procedimientos documentados de manera sistemática usando norma ISO 27001 que permitan minimizar los riesgos de seguridad.

Establecer los objetivos de control a implementar para la eficacia del SGSI en el ICBF centro zonal virgen y Turístico regional Bolívar.

Definir las políticas de seguridad informática que se deben implementar en la entidad basada en la norma ISO 27001.

4. MARCO DE REFERENCIA

4.1 MARCO TEÓRICO

La Seguridad de la información permite determinar que requiere ser protegido y porque, de que debe ser protegido y como protegerlo, se caracteriza por garantizar la Confidencialidad, Integridad y Disponibilidad de la información, basándose en el análisis, evaluación de riesgos y establecimiento de controles para mitigar el riesgo.[1]

El diseño de un Sistema de Gestión de Seguridad de la información permite a la empresa identificar las vulnerabilidades, las amenazas y los riesgos a los que están expuestos los activos, permitiendo establecer las normas o controles adecuados para proteger y respaldar los activos garantizando la continuidad de los procesos de la empresa.

Figura 1: SGSI

Fuente: www.iso27001.es

[1] PORTAL DE ISO 27001 EN ESPAÑOL, 28 de Agosto del 2015, [En línea] http://www.iso27000.es/download/doc_sgsi_all.pdf

El sistema de Gestión a diseñar en este proyecto estará basado en la norma ISO 27001:2013, la cual es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa, 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.[2]

Para el desarrollo de este proyecto se tuvo en cuenta diversas investigaciones referentes al tema, como el proyecto: Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la Ofrenda, realizado por Juan David Aguirre Cardona y Catalina Aristizabal Betancur en la Universidad Tecnológica de Pereira año 2013.

El proyecto Diseño del Sistema de Gestión de Seguridad de la Información que permita apoyar a la subgerencia de informática y tecnológica de la empresa telecomunicaciones de Bucaramanga en el proceso de certificación ISO 27001, realizado por Harrison Tamir Velazco, Universidad Pontifica Bolivariana, Floridablanca año 2008.

Por ultimo cabe mencionar el análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor del Cauca, realizado por Jhon Jairo Perafan Ruiz, Mildred Caicedo, Universidad Nacional Abierta y a Distancia, Popayán 2014.

[2] 27001 ACADEMY, QUE ES LA ISO 27001. Tomado el día 29 de Agosto. [En línea] http://advisera.com/27001academy/es/que-es-iso-27001/.

4.2 MARCO CONCEPTUAL

Información: Son todos los datos que maneja la empresa ya sea en forma digital o impresa. Se considera un activo de gran importancia por lo que requiere mayor protección.

Seguridad de la Información: Consiste en preservar la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.[3]

Los Activos: Son todos los elementos que posee una empresa como son: Los datos o información, servicios, aplicaciones (software), equipos (hardware), recursos físicos y recursos humanos.

Amenazas: Es cualquier situación que se puede presentar en la empresa dañando un activo de información, mediante la explotación de una vulnerabilidad.[3]

Vulnerabilidad: Son las debilidades que tiene una empresa, lo cual hace que se presenten amenazas a través de ellas.

Impacto: Es el daño que se produce en un activo cuando sucede una amenaza.

Los Controles: Son las medidas de protección que se implementan en una empresa para minimizar los riesgos.

[3] SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, Tomado el día 29 de Agosto del 2015, [En línea]. http://www.iso27000.es/download/doc_sgsi_all.pdf.

Políticas de Seguridad: Son parámetros o controles que permiten proteger los activos de información de una empresa.

Incidente de seguridad: Serie de eventos de seguridad no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones de la empresa.[3]

Gestión de activos: Busca proteger los activos de información, controlando el acceso solo a las personas que tienen permiso de acceder a los mismos.

Seguridad física: Trata principalmente de prevenir el acceso no autorizado a las instalaciones para prevenir daños o pérdidas de activos o hurto de información.

Sistema de Gestión de Seguridad de la Información (SGSI): Consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.[3]

Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización, el riesgo indica lo que le podría pasar a los activos si no se protegen adecuadamente.[4]

Análisis del Riesgo: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización.[4]

Riesgo Potencial: Es el daño probable de un activo cuando se encuentra desprotegido.

[4] JOSE LUIS QUINTERO, ANALISIS Y GESTIÓN DEL RIESGO. Tomado el día 30 de Agosto del 2015, [En línea] http://www.aec.es/c/document_library/get_file?uuid=b3945e58-17f2-4dc0-88ac-863ae9f998cb&groupId=10128.

Confidencialidad: Es la capacidad de no divulgar o publicar la información sensible de una empresa a personas no autorizadas.

Integridad: Es la característica de mantener la información de manera intacta o exacta sin tener modificación.

Disponibilidad: Consiste en tener los activos disponibles cuando se requieren de uso.

4.3 MARCO HISTÓRICO

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, Este estándar ISO 27001 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.[2]

4.3.1 EVOLUCIÓN DE LA ISO 27001: La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación, es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente, en el 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión, en el 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO, con algunos cambios, como estándar ISO 27001, fue revisada y actualizada la ISO 17799, lo cual quedo como ISO 27002:2005 el 1 de Julio de

2007, manteniendo el contenido así como el año de publicación formal de la revisión.[5]

En Marzo de 2006, posteriormente surgió la ISO 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.[5]

Asimismo, ISO ha continuado, el desarrollo de otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie.[5]

La última serie reciente es la publicación de las norma ISO/IEC 27001:2013, ISO/IEC 27002:2013 ambas aprobadas en la misma fecha: 25 de Septiembre de 2013.[5]

Figura 2: Resumen Histórico de la ISO 27001

Fuente: http://www.iso27000.es/

Los cambios que han traído la nueva norma ISO 27001: 2013 son varios, a continuación se mencionan los siguientes:

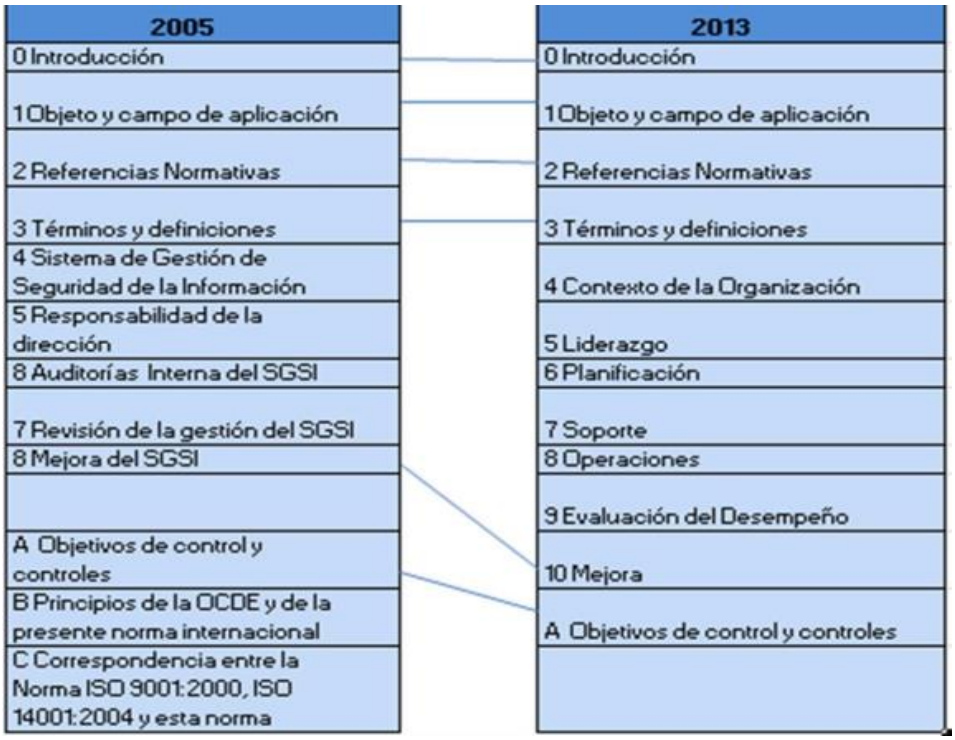
[5] ISO 27001, ORIGEN E HISTORIA. Tomado el día 31 de Agosto del 2015. [En línea] http://www.pmg-ssi.com/2013/12/iso27001-origen/

Las acciones preventivas se reemplazaron por “acciones para abordar los riesgos y oportunidades”.[6]

- Los requisitos de evaluación de riesgos son ahora más generales y se alinean con la norma ISO 31000.[6]
- Los requisitos de la declaración de aplicabilidad son similares pero se da mayor claridad en la determinación de los controles del proceso de tratamiento de riesgos.[6]
- Mayor énfasis en el establecimiento de los objetivos, el seguimiento del desempeño y métricas.[6]
- Mucho del texto de la versión 2005 y sus requerimientos permanecen, pero algunos se han movido a ajustarse a las nuevas secciones.[6]
- La norma ahora es menos descriptiva y prescriptiva.[6]
- Da mayores libertades en la implementación.[6]
- Propone un periodo de transición para las organizaciones ya certificadas.[6]
- Cambio en la terminología por ejemplo “política de SI” es usada en lugar de “política del SGSI”.[6]

[6] WILLIAM HALABY, CAMBIOS RESPECTO A ISO 27001:2013, CHARTER COLOMBIA. Tomado el día 31 de Agosto del 2015. [En línea]. http://isc2capitulocolombia.org/portal/images/documents/ISO_27001-2013_ISC2_Colombia_Chapter.pdf

Figura 3: Diferencia entre ISO 27001:2005 e ISO 27001:2013



Fuente: ISO 2701:2013 Nuevos cambios de la norma

4.4 MARCO LEGAL

Hoy en día existen muchas leyes que rigen la seguridad de la información, toda organización debe obligatoriamente cumplir con todas las leyes, normas, decretos, entre otros, que sean aplicables en el desarrollo de sus actividades. A continuación se describen un conjunto de normas que son aplicables al presente proyecto de grado.

LEY 1581 DEL 2012 Protección de Datos personales: pueden imponer las sanciones correspondientes a personas e instituciones tanto públicas como privadas que violen la confidencialidad, integridad y disponibilidad de los datos personales de terceros, también va a permitir una regulación a las bases de datos de todas las empresas, y lo que va a generar es que se garantice a todos los colombianos el derecho de acceder, actualizar y cancelar sus datos personales en el momento que desee.[7]

LEY 603 DE 2000: se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.[8]

La información es el activo más importante en el mundo actual, es por ello que el 17 de octubre de 2012 el Gobierno Nacional expidió la Ley Estatutaria 1581 de 2012 mediante la cual se dictan disposiciones generales para la protección de datos personales.

[7] CORPORACION COLOMBIA DIGITAL, LEY DE PROTECCION DE DATOS PERSONALES: Una Realidad en Colombia. Tomado el día 1 de Setiembre del 2013. [En línea] http://colombiadigital.net/actualidad/noticias/item/4778-ley-de-proteccion-de-datos-personales-una-realidad-en-colombia.html.

[8] LEYES INFORMATICAS EN COLOMBIA, UNAD. Tomado el día 14 de Abril del 2015, [En línea] http://gidt.unad.edu.co/leyesinformaticas.

5. METODOLOGIA

5.1 TIPO DE INVESTIGACIÓN

LINEA DE INVESTIGACIÓN: Teniendo en cuenta las líneas de investigación ofrecida por la escuela ECBTI (Escuela de Ciencias Básica, Tecnología e Ingenierías), para el desarrollo de este proyecto se aplicará **LA LÍNEA DE GESTIÓN DE SISTEMAS DEL ÁREA DE LA CIENCIAS DE LA COMPUTACIÓN**, el cual según Salazar (1999), está orientada a integrar, planificar y controlar los aspectos técnicos, humanos, organizativos, comerciales y sociales del proceso completo, empezando con el análisis del dominio del problema, continuando con el diseño de alternativas de solución y finalizando con la operatividad de un sistema. La idea de esta línea es que a partir conceptualización se pueda evaluar la situación actual y las perspectivas de los procesos para hacerlos más eficientes y dinámicos, a partir de la investigación aplicada, impulsada por la investigación inductiva y participativa.

5.2 MÉTODO

Los pasos a seguir en la investigación serán tomados en la siguiente manera:

- Definir el alcance del SGSI en cuanto al objetivo de la empresa, su localización, sus activos y tecnología.
- Definir una política de seguridad que incluya el marco general y los objetivos de seguridad de la información de la organización.

- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del riesgo, para este proyecto se usara la metodología MAGERIT, su objetivo es identificar los riesgos de información que tiene la empresa, realizando la identificación de los activos, análisis de vulnerabilidades, amenazas y la identificación de los objetivos de control a implementar para disminuir esos riesgos.

- Realizar el análisis y evaluación de riesgos, evaluar los impactos en los activos cuando ocurre una amenaza y los niveles de riesgos.

- Identificar y evaluar las distintas opciones de tratamiento de los riesgos aplicando los controles adecuados.

5.3 POBLACIÓN

El área de investigación se llevara a cabo en el interior de las oficinas el ICBF Centro Zonal Virgen y Turístico perteneciente a la regional Bolívar ubicado en el barrio Olaya Herrera en la ciudad de Cartagena.

5.4 ALCANCE

El estudio estará enfocado en las áreas de trabajo de las oficinas que tiene el Centro Zonal Virgen y Turístico del Instituto Colombiano de Bienestar Familiar perteneciente a la regional Bolívar, las cuales son Coordinación, secretaria, Recepción, área atención al ciudadano, rea de protección, área de prevención, área de recursos tecnológicos y archivo ubicado en el barrio Olaya Herrera de la Ciudad de Cartagena de Indias.

Estas oficinas cuentan con 25 empleados entre los cuales se tienen: Coordinador Abogados, Psicólogos, Nutricionistas, Trabajadoras sociales, secretarias, vigilantes y personal de aseo. Igualmente se cuenta con 17 oficinas, 15 equipos de cómputos, 3 impresoras en red, telefonía IP, escáner, un cuarto técnico con equipos de comunicaciones tales como Switch, Router, cámaras de seguridad y Patch panel.

6. ACTIVOS DE INFORMACIÓN

Los activos son todos los elementos presentes al interior de un sistema de información que tiene una organización, por lo tanto debe protegerse, tales como los datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos, administrativos, recursos físicos y recursos humanos[9].

Figura 4: Activos de Información.

Fuente: www.worldvisioncapacitacion.cl/wp-ontent/uploads/cursos_adjuntos/f52e0bd4c6c2c203413952826f916237.pdf

6.1 IDENTIFICACIÓN DE LOS ACTIVOS

Durante el desarrollo de este proyecto se encontraron los siguientes activos de información que se identificaron en el ICBF, Centro zonal Virgen y Turístico Regional Bolívar.

[9] ING. JOSE MANUEL POVEDA, ACTIVOS DE INFORMACIÓN, Modulo 7, ISO 27001. Tomado el día 24 de Julio del 2015. [En línea]. http://www.worldvisioncapacitacion.cl/wp-content/uploads/cursos_adjuntos/f52e0bd4c6c2c203413952826f916237.pdf

Tabla 1: Listado de Activos

TIPO DE ACTIVOS	NOMBRE	CARACTERISTICAS
COMUNICACIONES [COM]	Switch	Marca 3Com, modelo 4200g, número de puertos 48.
	Rack	Existe un Rack con capacidad para 6 switches, en la actualidad hay 2.
	Router	Marca CISCO 1811, tipo fibra óptica.
HARDWARE [HD]	Impresoras	HP Laser 4250 conectada en red total 3.
	UPS	Marca Powerware, capacidad 6KVA,
	Telefonía IP	Marca Asteric.
	Computadores	Marca Lenovo, HP 5057, Dell Optiplex, equipos de escritorios, 1 portátil,
	Escáner	Marca Epson SX10.
SOPORTE DE INFORMACIÓN FISICA	Documentos impresos en papel.	.La documentación física de los procesos de todos los servicios que presta el ICBF dentro de los cuales se tiene: Procesos de protección, prevención, restablecimiento de derecho, Adopciones, Responsabilidad penal, nutrición, Contratación, Liquidación de hogares.
INFORMACIÓN DIGITAL [ID]	Documentos en Word, Excel y PDF de los servicios que prestan	.La Información Digital de los procesos de todos los servicios que presta el ICBF dentro de los cuales se tiene: Procesos de protección, prevención, restablecimiento de derecho, Adopciones, Responsabilidad penal, nutrición, Contratación, Liquidación de hogares.
PERSONAL [P]	Usuarios Internos (Empleados) y usuarios externos (clientes)	Coordinadores, Equipo Psicosocial (nutricionistas, psicólogas, defensores de familia, trabajo social) grupo financiero, Secretaria, Archivo, Personal aseo, vigilantes.
SOFTWARE [SF]	Aplicaciones Web.)	Sistema de Información Misional SIM: www:sim.icbf.gov.co/sim versión 2.0
	Sistemas Operativo	Windows 7. Profesional
	Correo electrónico	Microsoft Outlook 2010
	Antivirus, Navegadores Web.	Microsoft Forefront; Internet Explorer 9.

Fuente: El Autor

6.2 DIMENSIONES DE LOS ACTIVOS.

Una vez identificados los activos, se procede a realizar la valoración para estimar qué valor tiene cada activo para la organización, según su importancia, para ello se definen las dimensiones o los criterios por los cuales se van a evaluar, los criterios de evaluación son los siguientes:

[C] Confidencialidad: Cuanto daño hace a la empresa si se publica su información confidencial.

[I] Integridad: Si el activo es modificado, que daño causaría a la empresa.

[D] Disponibilidad**:** Cuando se necesite el activo y no esté disponible, cuanto perjuicio causaría esta situación a la empresa.

[T] Trazabilidad: Si no se sabe quién accede al activo y que acciones realiza, se evalúa el daño que esta situación causaría a la empresa.

[A] Autenticidad: Saber si el activo no es propio de la persona, qué perjuicio causaría no saber si el activo es propio de la persona.

Tabla 2: Valoración de la Confidencialidad de Activos.

VALOR CUANTITATIVO	VALOR CUALITATIVO	CRITERIO
10	Muy Alto	La divulgación del activo causaría daños catastróficos, daño a la reputación y la imagen de la organización se verían comprometidas.
8-9	Alto	La divulgación del activo causaría daños en un 80 y 90%.
5-7	Medio	La divulgación del activo causaría daños en un 50 y 70%.
3-4	Bajo	La divulgación del activo causaría daños en un 30 y 40%.
1-2	Muy Bajo	La divulgación del activo causaría daños en un 10 y 20%

Fuente: el autor.

Tabla 3: Valoración de la Disponibilidad de Activos.

VALOR CUANTITATIVO	VALOR CUALITATIVO	CRITERIO
10	Muy Alto	El activo debe estar disponible al menos el 100% del tiempo.
8-9	Alto	El activo debe estar disponible entre el 80 y 90% del tiempo.
5-7	Medio	El activo debe estar disponible entre el 50 y 70 % del tiempo.
3-4	Bajo	El activo debe estar disponible entre el 30 y40% del tiempo.
1-2	Muy Bajo	El activo debe estar disponible entre el 10 y20% del tiempo

Fuente: el autor

Tabla 4: Valoración de la Integridad de Activos.

VALOR CUANTITATIVO	VALOR CUALITATIVO	CRITERIO
10	Muy Alto	El activo tiene que estar correcto y completo al menos en un 100%
8-9	Alto	El activo tiene que estar correcto y completo al menos en un 80 y90%
5-7	Medio	El activo tiene que estar correcto y completo al menos en un 50 y70%
3-4	Bajo	El activo tiene que estar correcto y completo al menos en un 30 y40%
1-2	Muy Bajo	El activo tiene que estar correcto y completo al menos en un 10 y20%

Fuente el autor

Tabla 5: Valoración de la Trazabilidad de Activos.

VALOR CUANTITATIVO	VALOR CUALITATIVO	CRITERIO
10	Muy Alto	El activo realiza la trazabilidad al 100%
8-9	Alto	El activo realiza la trazabilidad el menos en un 80 %
5-7	Medio	El activo realiza la trazabilidad el menos en un 50 y 70 %
3-4	Bajo	El activo realiza la trazabilidad el menos en un 30 y 40%
1-2	Muy Bajo	El activo realiza la trazabilidad el menos en un 10 y 20 %

Fuente el autor

Tabla 6: Valoración de la Autenticidad de Activos.

VALOR CUANTITATIVO	VALOR CUALITATIVO	CRITERIO
10	Muy Alto	El activo es 100% propio de la persona.
8-9	Alto	El activo es propio de la persona en un 80 y 90 %
5-7	Medio	El activo es propio de la persona en un 50 y 70%
3-4	Bajo	El activo es propio de la persona en un 30 y 40%
1-2	Muy Bajo	El activo es propio de la persona en un 10 y 20%

Fuente el autor

6.3 VALORACIÓN DE LOS ACTIVOS.

Un activo puede ser evaluado según sus diferentes dimensiones. En la siguiente tabla se evalúa cada uno de los activos de la empresa en cada una de sus dimensiones para saber cada valor.

Tabla 7: Valoración de los Activos según sus Dimensiones.

ACTIVOS	DIMENSIONES				
	D	I	C	T	A
COMUNICACIONES					
Rack	8	5	5	4	4
Switch	10	9	9	9	9
Router	10	10	10	9	9
HARDWARE					
Computadores	10	10	10	9	9
Impresoras	9	8	8	8	8
Escáner	6	6	6	6	6
Telefonía IP	8	7	6	5	5
UPS	9	8	8	8	8
SOFTWARE					
Sistema Operativo	10	10	9	9	10
Aplicativo Web.	10	10	10	9	10
Antivirus	9	8	7	7	7
Navegadores Web	9	9	8	7	8
Correo electrónico	10	9	10	9	9

INFORMACIÓN FISICA					
Documentos físicos de información de todos los procesos de la empresa.	10	10	10	9	9
INFORMACIÓN DIGITAL					
Información Digital que se maneja en el PC.	10	10	9	9	9
PERSONAL					
Coordinación	9	7	7	8	8
Secretaria	8	8	7	7	7
Psicología	9	8	8	7	7
Nutrición	9	8	8	7	7
Trabajo Social	9	8	8	7	7
Defensor de Familia	9	8	8	7	7
Vigilantes	9	8	8	7	7

Fuente el Autor

6.4 CLASIFICACIÓN DE ACTIVOS.

- **USO PÚBLICO:** Información que está a disposición de cualquier persona.

  USO INTERNO: Información cuya divulgación no causa daños serios a la empresa, su acceso es libre para los funcionarios a través de la intranet o de cualquier otro medio.

- **USO CONFIDENCIAL:** Información de uso privado para la empresa, puede afectar considerablemente la empresa si se llegaría a conocer por personal no autorizado, para divulgar esta información se requiere de la aprobación de su respectivo propietario.

- **USO SECRETO:** Información que sólo puede ser conocida y utilizada por un grupo muy reducido de funcionarios, usada por los dueños del proceso.

6.5 INVENTARIO DE ACTIVOS.

El inventario de activos es la base para la gestión de los mismos, ya que tiene que incluir toda la Información necesaria para mantenerlos operativos e incluso poder recuperarse ante un desastre, esta información está conformada por:

- Identificación del activo: Un código para ordenar y localizar los activos.
- Tipo de activo: A qué categoría pertenece el activo.
- Propietario**:** Quien es la persona a cargo del activo.
- Localización**:** Dónde está físicamente el activo, en el caso de información en formato electrónico, en qué equipo se encuentra.
- Atributos**:** Clasificar el activo de acuerdo a su dimensión.

Tabla 8: Listado de Inventario de Activos

IDENTIFICADOR				PROPIEDAD		LIDER	_ATRIBUTOS				CLASIFICACION DE ACTIVOS DE INFORMACIÓN	
PROCESO	**AREA**	**ACTIVO DE INFORMACIÓN**	**TIPO**	**PROPIETARIO**	**UBICACIÓN**	**NOBRE PROPIETARIO**	**C**	**I**	**D**		**CLASIFICACION**	**MISIONAL**
Gestión de Restablecimiento de Derecho.	gestión para la prevención y protección	Resolución de situación de adaptabilidad	DIG – FIS	Defensora de Familia	Dependencia de Protección	Libia Espinosa, Coordinadora del centro zonal.	MA	A	MA		CONFIDENCIAL	SI
Gestión de Restablecimiento de Derecho.	gestión para la prevención y protección	Asuntos Conciliables	DIG – FIS	Defensora de Familia	Dependencia de Protección	Libia Espinosa, Coordinadora del centro zonal.	A	A	A		CONFIDENCIAL	SI
Gestión de Restablecimiento de Derecho.	gestión para la prevención y protección	Asuntos no Conciliables	DIG– FIS	Defensora de Familia	Dependencia de Protección	Libia Espinosa, Coordinadora del centro zonal.	MA	A	A		CONFIDENCIAL	SI
Gestión de Restablecimiento de Derecho.	gestión para la prevención y protección	Procesos de Adopciones	DIG y FIS	Defensora de Familia	Dependencia de Protección	Libia Espinosa, Coordinadora del centro zonal.	MA	MA	A		CONFIDENCIAL	SI
Gestión de Restablecimiento de Derecho.	gestión para la prevención y protección	Resultado prueba de ADN	INF – FIS	Defensora de Familia	Dependencia de Protección	Libia Espinosa, Coordinadora del centro zonal.	MA	MA	MA		RESERVADA	SI
Gestión para la Nutrición	gestión para la prevención y protección	Valoración medica (pediátrica, nutricional, medicina legal, psicológica	INF – FIS	Equipo Psicosocial.	Dependencia de Prevención	Libia Espinosa, Coordinadora del centro zonal.	A	M	M		USO INTERNO	SI
Gestión para la Nutrición	gestión para la prevención y protección	FORMATO FT1 RECUPERACION NUTRICIONAL	INF – FIS	Nutricionista.	Dependencia de Prevención	Libia Espinosa, Coordinadora del centro zonal.	M	M	M		USO INTERNO	SI

Gestión para la Nutrición	Gestión para la Prevención	ft1 formato de desayunos infantiles con amor	DIG	Nutricionista	Dependencia de Prevención	Libia Espinosa, Coordinadora del centro zonal.	M	B	B		USO INTERNO	SI
Gestión para la Nutrición	Gestión para la Prevención	minuta patrón cdi	DIG	Nutricionista	Dependencia de Prevención	Libia Espinosa, Coordinadora del centro zonal.	M	B	B		CONFIDENCIAL	SI
Gestión para la Nutrición	Gestión para la Prevención	Formatos de novedades del programa de día.	DIG	Nutricionista	Dependencia de Prevención	Libia Espinosa, Coordinadora del centro zonal.	M	M	M		USO INTERNO	SI
Gestión para la Nutrición	Gestión para la Prevención	programación de visitas PARD	DIG	Nutricionista	Dependencia de Prevención	Libia Espinosa, Coordinadora del centro zonal.	M	M	M		CONFIDENCIAL	SI
Gestión de Restablecimiento de Derecho	Gestión para la Prevención	informe de seguimiento	INF – FIS	Equipo psicosocial	Dependencia de Prevención y protección.	Libia Espinosa, Coordinadora del centro zonal.	M	M	M		USO INTERNO	SI
Gestión para la Atención Integral de la Primera Infancia.	Gestión para la Prevención y Protección.	formatos de supervisión y orientación, seguimiento cdi institucional y familiar	INF – FIS	Equipo psicosocial	Dependencia de Prevención y protección.	Libia Espinosa, Coordinadora del centro zonal.	M	M	M		CONFIDENCIAL	SI
Gestión para la Atención Integral de la Primera Infancia.	Gestión para la Prevención y Protección.	valoración Psicológicas	DIG	Gestión para la Nutrición	Dependencia de Prevención y protección.	Libia Espinosa, Coordinadora del centro zonal.	M	M	A		USO INTERNO	SI
Gestión de Información y Tecnología.	Planeación y Sistemas	Switch (1)	HW	Ingeniero Regional	Área de Información y Tecnología	Libia Espinosa, Coordinadora del centro zonal.	MA	MA	MA		USO INTERNO	SI
Gestión de Información y Tecnología.	Planeación y Sistemas	Router (1)	HW	Ingeniero Regional	Área de Información y Tecnología	Libia Espinosa, Coordinadora del centro zonal.	MA	MA	MA		USO INTERNO	SI

Gestión de Información y Tecnología.	Planeación y Sistemas	UPS (1)	HW	Ingeniero Regional	Área de Información y Tecnología	Libia Espinosa, Coordinadora del centro zonal.	MA	MA	MA		USO INTERNO	SI
Gestión de Restablecimiento de Derecho.	Gestión para la Prevención y Protección	Acta de Colocación Familiar PARD	INF – FIS	Equipo Psicosocial	Oficina de Prevención y Protección	Equipo Psicosocial	M	A	M		USO INTERNO	SI
Gestión de Restablecimiento de Derecho	Gestión para la Prevención y Protección	Informe integral del niño	INF – FIS	Equipo Psicosocial	Oficina de Prevención y Protección	Equipo Psicosocial	MA	A	A		CONFIDENCIAL	SI
Gestión de Restablecimiento de Derecho.	Gestión para la Prevención y Protección	Acta de equipo técnico	INF – FIS	Equipo Psicosocial	Oficina de Prevención y Protección	Equipo Psicosocial	M	A	M		USO INTERNO	SI
Gestión de Restablecimiento de Derecho.	Gestión para la Prevención y Protección	Acta de reintegro familiar	INF – FIS	Equipo Psicosocial	Oficina de Prevención y Protección	Equipo Psicosocial	M	A	A		USO INTERNO	SI
Gestión de Restablecimiento de Derecho.	Gestión para la Prevención y Protección	Boleta de Ingreso	INF – FIS	Atención al ciudadano	Oficina de Prevención y Protección	Equipo Psicosocial	B	M	B		USO INTERNO	SI
Gestión de Restablecimiento de Derecho.	Gestión para la Prevención y Protección	Informe institucional / hogar sustituto del niño	DIG	Defensora de Familia	Oficina de Prevención y Protección	Equipo Psicosocial	M	A	M		USO INTERNO	SI
Gestión de Restablecimiento de Derecho.	Gestión para la Prevención y Protección	Demanda	INF – FIS	Defensora de Familia	Oficina de Prevención y Protección	Equipo Psicosocial	A	A	A		USO INTERNO	SI

Fuente el Autor

7. MEDIDAS DE SEGURIDAD

Actualmente la empresa cuenta servicio de guardias en la entrada permanentemente, en horarios laborales y no laborales, se ubican en el interior y en el exterior del centro zonal.

En el cuarto de cableado donde están los equipos de comunicaciones se cuenta con el aviso de prohibido la entrada a personal no autorizado, las oficinas cuentan con puertas, se deben registrar los elementos informáticos ajenos a la institución a la entrada del centro zonal.

7.1 MEDIAS DE SEGURIDAD EXISTENTES.

- En el cuarto de cableado donde están los equipos de comunicaciones tienen aviso de prohibido la entrada a personal no autorizado.
- Los equipos de la empresa se encuentran protegidos por software de detección y reparación de virus, mensualmente se publican las estadísticas de virus como forma de concienciación.
- Sistemas de prevención contra intrusos (Firewall)
- La regional Bolívar cuenta con un sistema de detector de vulnerabilidades (Netclarity) que previene frente acciones forzosas o no autorizadas.
- En la entrada del centro zonal tienen una planilla de ingreso para el registro de elementos ajenos a la institución el cual es controlada por el vigilante.
- El sistema del correo electrónico tiene un Anti spam para controlar el ingreso de correos no deseados y propagación de virus.

- En el cuarto de archivo se debe registrar los préstamos de las carpetas de las historias de los niños.
- En el cuarto de cableado tienen una Bitácora de acceso para registrar el ingreso de las personas que entran al cuarto.
- La información contenida en memorias USB es encriptado para evitar la fuga de información, con un aplicativo que se llama Bitlocker.

8. ANALISIS DE VULNERABILIDADES

Una vulnerabilidad se define como un estado de debilidad que al ser explotado afecta el estado de los activos de la empresa.[10]

Existen diferentes tipos de Vulnerabilidades, entre las cuales se mencionan:

- Natural: Se presentan principalmente en deficiencias, por ejemplo no disponer de reguladores, no-Break, mal sistema de ventilación o calefacción.[10]

- Física: Se refiere a la posibilidad de entrar o acceder físicamente al sistema para robar, modificar o destruirlo.[10]

- Medios o Dispositivos: Se refiere a la posibilidad de robar o dañar los discos, cintas, listados de impresora, etc.[10]

- Hardware: Fallas en las piezas físicas (ya sea por mal uso, descuido, mal diseño etc.) dejando al sistema desprotegido o inoperable.[10]

- Software: Deficiencias en el funcionamiento del software. Ejemplo: controles de acceso, antivirus desactualizado, correos no deseados etc.[10]

- Factor humano: Negligencia en el seguimiento de las políticas de seguridad, y mal uso del equipo de cómputo. Robo de información o la destrucción de los sistemas.[10]

-

[10] RIESGOS Y CONTROL INFORMATICO, Lección 1, UNAD. Conceptos de Vulnerabilidad, Riesgos y Amenazas. Tomado el día 16 de Julio del 2015. [En línea] http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

8.1 VALORACIÓN DE VULNERABILIDAD.

Las vulnerabilidades deben valorarse y priorizarse, pero se deben identificar claramente y evaluarlas tomando como criterios la frecuencia de ocurrencia.[10]

Tabla 9: Matriz de Valoración de Vulnerabilidad

Valor cuantitativo	Frecuencia	Descripción	Probabilidad
10	Muy Alta	A Diario.	90– 100%
8-9	Alta	Cada Semana	60 – 80%
5-7	Media	Cada Mes	30% - 60%
3-4	Bajo	Cada Año	10% - 30%
1-2	Muy Bajo	Cada varios años	0 -10%

Fuente el autor

Tabla 10: Identificación y Valoración de las vulnerabilidades

CATEGORIA	ACTIVOS	VULNERABILIDADES	VALOR	PROBABILIDAD
HARDWARE	Infraestructura tecnológica y/o de comunicaciones de la Empresa.	El activo está expuesto a la humedad.	4	30%
		Incumplimiento en la ejecución del plan de mantenimiento preventivo de dispositivos activos.	3	30%
		Se encuentran ubicados en sitios con poca visibilidad	4	30%
		El cuarto de cableado se encuentra sin extintor.	4	30%
		Con poca frecuencia se realizan labores de limpieza.	5	30%
	Rack, Switch, Router, UPS	No existencia de sistemas de controles de acceso al cuarto de cableado.	6	40%
		No se cuenta con un sistema de energía eléctrica de contingencia (Planta en caso de caídas del servicio de energía.	2	20%
		La ups presenta fallas técnicas.	6	40%

		Rack sin seguridad (sin llaves)	5	30%
HARDWARE	Recursos Tecnológicos y Auxiliares Computadores, Impresoras, Escáner, Telefonía IP. Aire Acondicionado	No se realiza escaneo de las memorias para determinar si poseen virus.	6	40%
		Frecuentes fallas en el funcionamiento del activo.	5	30%
		Se obtiene fácil acceso a la BIOS, lo que ocasiona que otras personas puedan modificar la configuración.	2	20%
		El administrador del sistema no realiza chequeos rutinarios o periódicos, solo revisa los equipos ante problemas reportados por los funcionarios.	5	45%
		Dejan equipos desatendidos, facilitando el ingreso de otras personas.	6	45%
		Los equipos cuentan con USB, dando origen a posibles fugas de información.	6	45%
		Uso de los activos para fines personales.	8	60%
		Prestamos de equipos.	6	40%
		Hurto de dispositivos o de medios de comunicación.	3	30%
		Incumplimientos por parte de los proveedores frente a las garantías de los equipos.	3	20%
		No se realizan mantenimientos preventivos con frecuencia.	7	45%
		No se realiza un uso correcto del activo.	4	30%
		El activo está expuesto al polvo.	5	40%
	Sistemas informáticos de la empresa. Sistemas Operativo Aplicaciones	Uso del correo institucional para uso personal.	6	40%
		No existen roles en la creación de las cuentas.	3	20%
		No se descargan los parches de seguridad con regularidad.	2	10%
		Mala configuración de los sistemas informáticos.	5	30%
		Ingreso a páginas no permitidas tales como Hotmail, Facebook, descarga de música entre otras.	5	40%

SOFTWARE	Web. Correo Electrónico Antivirus. Navegadores Web.	No se realizan correctamente los mantenimientos.	3	30%
		Las contraseñas de autenticación no son seguras, no son cambiadas con frecuencia.	7	45%
		Manejo inadecuado de Hardware y software.	6	40%
		Los usuarios no cuentan con capacitación para el manejo del activo.	3	30%
		No se finaliza correctamente la sesión.	6	40%
Activos de Información	Información física. (Documentos) Información Digital.	No realizan copias de seguridad, periódicamente.	3	30%
		Información digital de fácil acceso, equipos desatendidos sin bloquear.	6	40%
		Activos físicos sobre el escritorio, los documentos.	6	50%
		Fácil ingreso a las oficinas.	2	30%
		Los archivadores de documentos están ubicados en zona de humedad.	3	10%
		Se dejan documentos sobre la impresora.	6	40%
Recurso Humano	Directivos, Empleados y Vigilantes.	Asignación de equipos a otra persona en vacaciones.	6	40%
		Falta Interés por aplicar las políticas de seguridad.	6	40%
		Insuficiencia de personal destinado al soporte.	5	30%
		Falta de sensibilización a los funcionarios sobre la importancia de las políticas de seguridad.	6	40%
		Incumplimiento de las medidas de seguridad.	4	60%
		Resistencia al cambio y al aprendizaje de las nuevas tecnologías.	3	40%

Fuente el autor.

9. GESTIÓN DEL RIESGO

El Desarrollo de esta etapa consta de dos partes:

- Análisis de riesgos: Se realiza mediante la metodología MAGERIT, se determina que riesgos posee la organización y estimar el impacto. [11]

- Tratamiento de los riesgos: Consiste en aplicar medidas de protección basadas en objetivos de control.

En el Análisis de riesgos se determina cómo es, cuánto vale y cómo se encuentra protegido el sistema, para realizar este análisis se considera los siguientes elementos a tratar que son: Los activos, las amenazas y los controles.[11]

En esta etapa se requiere realizar el Análisis de Riesgos el cual consta de varios pasos mencionados a continuación.[11]

- Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio que valga su degradación o daño de él.

- Determinar a qué amenazas están expuestos aquellos activos.

- Determinar qué salvaguardas o controles son eficaces frente al riesgo.

- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

[11] MAGERIT V 3.0, Metodología de Análisis y Gestión de los Sistemas de Información, Tomado el día 15 de Julio del 2015. [En línea] http://es.slideshare.net/kinny32/magerit-v3-libro1metodo.

9.1 IDENTIFICACIÓN DE LAS AMENAZAS.

Las Amenazas son cualquier situación que se presenta causando daños a los activos de información, todo esto gracias a la explotación de las vulnerabilidad al interior de la organización.

Las Amenazas están clasificadas en cuatro grupos las cuales son:

[N] Desastres naturales: Inundaciones, Tormentas eléctricas, terremotos, Variaciones en los voltajes de la energía.

[I] De origen industrial: Errores en los dispositivos, daño en los equipos.

[E] Errores y fallos no intencionados:

[A] Ataques Intencionados: Curiosos, Intrusos remunerados, Terroristas, Robo, Sabotaje, Ingeniería social.

Tabla 11: Identificación Amenazas de Desastres Naturales.

AMENAZA	DESCRIPCION
[N] Fuego	Incendio: Posibilidad de que el fuego acabe con los recursos del sistema.
[N] Daños por Agua	Inundaciones: posibilidad de que el agua acabe con recursos informáticos.
[N]Desastres Naturales	Incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.

Fuente: www.udistrital.edu.co:8080/documents/276352/356568/Cap5GESTIÓN Riesgo.pdf

Tabla 12: Identificación Amenazas de Origen Industrial**.**

AMENAZA	DESCRIPCION
[I] Contaminación Medioambiental.	Vibraciones, polvo, suciedad.
[I] Avería de origen Físico o lógico.	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
[I] Corte del suministro eléctrico.	Cese de la alimentación de potencia
[I] Condiciones inadecuadas de temperatura y/o humedad.	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad.
[I]Fallos de servicios de comunicación	Cese de la capacidad de transmitir datos de un sitio a otro.
[I] Degradación de los soportes de almacenamiento de la información.	Como consecuencia del paso del tiempo.

Fuente: www.udistrital.edu.co:8080/documents/276352/356568/Cap5GESTIÓN Riesgo.pdf

Tabla 13: Identificación Amenazas de Errores y fallos no intencionados

AMENAZA	DESCRIPCIÓN
[E] Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, d atos, etc.
[E] Errores mantenimiento y actualización de Software.	El administrador realiza mantenimiento y erróneamente realiza operaciones equivocadas.
[E] Errores de mantenimiento y actualización de Hardware.	Errores en los procedimientos de los procesos de actualización,
[E] Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas.
[E] Alteración accidental de la información	Alteración accidental de la información.
[E] Destrucción de información	Pérdida accidental de información.
[E] Divulgación de información.	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel.
[E]Caída del sistema por agotamiento de recursos.	La carencia de recursos suficientes provoca la caída del siste ma cuando la carga de trabajo es desmesurada.
[E] Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público.
[E] Errores de Administrador.	Son las equivocaciones que comenten los administradores a la hora de realizar una instalación u operación con el dispositivo.

Fuente: www.udistrital.edu.co:8080/documents/276352/356568/Cap5GESTIÓN Riesgo.pdf

Tabla 14: identificación de Amenazas de Ataques Intencionados

AMENAZAS	DESCRIPCION
[A] Suplantación de la identidad del usuario.	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines prop ios.
[A] Abuso de privilegios de acceso.	Cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia hay problemas.
[A] Uso no previsto.	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales En internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
[A] Daño por manipulación de usuario.	Falta de conciencia del buen uso de los equipos informáticos.
[A] Difusión de software dañino.	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
[A] Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin estar autorizado.
[A] Modificación de la información	Alteración intencional de la información, con ánimo de obtener u n beneficio o causar un perjuicio.
[A] Destrucción la información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.
[A] Divulgación de información	Revelación de información.
[A] Manipulación de programas	Alteración intencionada del funcionamiento de los programas.
[A] Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[A] Robo	La sustracción de equipamiento provoca directamente la carenci a de un medio para prestar los servicios es decir una indisponibilidad.
[A] Indisponibilidad del persona	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los acceso s.
[A] Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
[A] Ingeniería social	Abuso de la buena fe de las personas para que realicen activida des que interesan a un tercero.

Fuente: www.udistrital.edu.co:8080/documents/276352/356568/Cap5GESTIÓN Riesgo.pdf

9.2 VALORACIÓN DE LAS AMENAZAS.

Una vez determinado las amenazas, se procede a valorar su influencia en el valor del activo, su objetivo es:

- Evaluar la probabilidad para saber cuán probable o improbable es que se materialice la amenaza.[11]

- Estimar la degradación que causaría la amenaza en cada activo si llegara a materializarse, para saber cuán perjudicado resultaría el valor. [11]

Tabla 15: Valor de Amenazas

MA	MUY ALTA	10
A	ALTA	8-9
M	MEDIA	5-7
B	BAJA	3-4
MB	MUY BAJA	1-2

Fuente el Autor.

Tabla 16: Probabilidad de ocurrencia.

Valor cuantitativo	**Frecuencia**	**Descripción**	**Probabilidad**
10	Muy Alta	A Diario	80 – 100%
8-9	Alta	Cada Semana	50 – 70%
5-7	Media	Cada Mes	30 % - 50 %
3-4	Bajo	Cada Año	15% - 30%
1-2	Muy Bajo	Cada varios años	0 -10 %

Fuente el Autor

9.3 VALORACIÓN DEL IMPACTO

El impacto es el daño causado a la empresa cuando sucede una amenaza sobre un activo de información, Este se calcula en la siguiente tabla de acuerdo a la fórmula:

Impacto = Valor del Activo * Degradación.[11]

9.4 VALORACIÓN DE RIESGOS.

Se calcula el Riesgo, el cual es la probabilidad de ocurrencia de la amenaza por el impacto causado, su fórmula es la siguiente:

Riesgo: Impacto * Probabilidad.[11]

Para realizar esta etapa, como primer lugar se tiene la identificación de los activos, segundo la identificación de cada amenaza sobre cada activo, y por último se tiene el cálculo del Impacto que ocasiona a la organización cuando ocurre una amenaza, gracias a esos resultados obtenidos por cada uno de estos pasos se puede llevar a cabo la valoración de los riesgos, el nivel de riesgo se divide en cuatro zonas:

- Bajo: El nivel de riesgo es bajo, y por lo tanto pueda que no se tomen acciones para evitarlo.
- Medio: El nivel de riesgos es medio, se somete a estudio para su debido tratamiento.
- Alto: El nivel de riesgo es alto, se requiere atención, es necesario implantar los controles para mitigar los riesgos.
- Crítico: El nivel de riesgo es crítico, es decir es preocupante para la organización porque se deben urgentemente implantar controles para minimizarlos.

Tabla 17: Valoración de las Amenazas, Cálculo de Impacto y Riesgos.

ACTIVOS	AMENAZAS	PROBAB-ILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
COMUNICACIONES									
Rack	[N] Daños por agua.	3	2	10	8	3	5	10 * 9 = 90	90 * 3 = 270
	[N] Desastres naturales.	3	3	10	4	5	7	10 * 10 = 100	100 * 3 = 300
	[I] Condiciones inadecuadas de temperatura y/o humedad.	3	1	6	4	3	3	10 * 7 = 70	70 * 4= 280
	[I] Contaminación Medioambiental.	4	2	6	3	3	2	10 * 7 = 70	70 * 4= 280
	[N] Fuego	1	5	10	5	6	4	10 * 10 = 100	100 * 1= 100
	[I] Avería de origen Físico o lógico	2	2	7	3	3	4	10 * 9 = 90	90 * 2 = 180
	[A] Abuso de privilegios de acceso.	2	4	8	5	3	3	10 * 10 = 100	100 * 2= 200
	[A] Acceso no autorizados.	5	6	8	4	5	3	10*10=100	100 * 5=500
Switch	[N] Fuego.	1	6	10	5	6	8	10*10= 100	100 * 1= 100
	[N] Daños por agua.	3	2	10	8	3	5	10 * 10 = 100	100* 3 = 300
	[N] Desastres naturales.	3	3	10	8	6	7	10 * 10 = 100	100* 3 = 300
	[I] Condiciones inadecuadas de temperatura y/o humedad.	4	2	10	5	4	4	10 * 9 = 90	90 * 4 = 360
	[I] Contaminación Medioambiental.	3	5	9	6	5	4	10 * 8 = 80	80* 3 = 240
	[I] Avería de origen Físico o lógico.	2	6	10	7	8	5	10 * 10 = 100	100 * 2= 200
	[A] Acceso no autorizados.	3	10	10	8	6	8	10 * 9 = 100	100 * 3= 300
	[I]Caída del sistema por agotamiento de recursos.	3	5	10	5	6	5	10 * 10 = 100	100 * 3= 300
	[I] Denegación del servicio.	2	6	10	5	9	8	10 * 10 = 100	100 * 2= 200
	[I] Corte del suministro eléctrico.	4	4	10	5	4	5	10 * 10 = 100	100*4= 400
	[I]Fallo de servicio de comunicaciones.	3	7	10	5	4	5	10 *10 =100	100*3= 300
	[E] Errores de Administrador.	2	8	10	6	7	8	10 * 10 = 100	100*2= 200
	[A] Robo.	1	5	10	6	4	10	10*10=100	100*1=100
	[A] Abuso de privilegios de acceso.	2	10	10	10	7	8	10 * 10 = 100	100*2= 200

Router	[I] Denegación del servicio.	2	9	10	9	7	8	10 * 10 = 100	100*2=200
	[N] Daños por agua.	3	4	10	4	4	5	10 * 10 = 100	100* 3 = 300
	[N] Desastres naturales.	3	4	10	5	4	8	10 * 10 = 100	100* 3 = 300
	[I] Condiciones inadecuadas de temperatura y/o humedad.	3	3	10	5	4	3	10 * 10 = 100	100* 3= 300
	[I] Contaminación Medioambiental.	3	4	8	6	4	5	10 * 9 = 90	90* 3 = 270
	[A]Robo.	1	7	10	8	6	8	10*10=100	100*1=100
	[I] Avería de origen Físico o lógico	2	5	10	6	4	4	10 * 10 = 100	100*2=200
	[N] Fuego.	1	6	10	8	7	8	10*10= 100	100 * 1= 100
	[A] Acceso no autorizados.	3	8	9	8	7	6	10 * 10 = 100	100*3= 300
	[I] Corte del suministro eléctrico	4	5	10	6	4	5	10 * 10 = 100	100*4=400
	[I]Caída del sistema por agotamiento de recursos.	3	5	10	5	6	5	10 * 10 = 100	100*3=300
	[I] Fallo de servicio de comunicaciones.	3	7	10	8	7	6	10 *10 =100	100*3=300
	[E] Errores de Administrador.	2	8	10	9	8	8	10 * 10 = 100	100*2=200
	[A] Abuso de privilegios de acceso.	2	9	10	9	7	8	10 * 10 = 100	100*2=200
HARDWARE									
Computadores	[A] Robo de hardware.	1	10	10	8	7	6	10 * 10 = 100	100*1=100
	[N] Daños por agua.	3	4	10	4	5	5	10 * 10 = 100	100* 3 = 300
	[N] Desastres naturales.	3	6	10	5	6	8	10 * 10 = 100	100* 3 = 300
	[I]Condiciones inadecuadas de temperatura y/o humedad.	3	4	10	4	5	7	10 * 10 = 100	100* 3= 300
	[I] Contaminación Medioambiental.	4	3	10	4	6	5	10 * 10 = 100	100*4 =400
	[A] Modificación de la información	5	10	10	10	8	7	10*10=100	100*5=500
	[A]Suplantación de la identidad del usuario.	5	10	10	10	8	8	10*10=100	100*5=500
	[I] Avería de origen Físico o lógico.	5	8	10	7	8	9	10 * 10 = 100	100*5=500
	[N] Fuego.	1	8	10	9	8	8	10 * 10 = 100	100 * 1 = 100

	[E] Errores de mantenimiento y actualización de Hardware.	3	9	10	9	7	8	10 * 10 = 100	100 * 3 = 300
	[A] Acceso no autorizados.	6	10	10	8	8	8	10 * 10 = 100	100*6= 600
	[A] Uso no previsto.	7	5	9	4	5	6	10*8=80	80 * 7 =560
	[I] Corte del suministro eléctrico.	4	10	10	8	7	6	10 * 10 = 100	100*4=400
	[E] Errores de Administrador.	3	9	10	9	8	8	10 * 10 = 100	100 * 3 = 300
	[A] Daño por manipulación de usuarios.	5	8	10	9	7	8	10 * 10 = 100	100 * 5 = 500
	[A] Abuso de privilegios de acceso.	5	9	8	9	8	8	10 * 10 = 100	100 * 5 = 500
	[A] Divulgación de la información.	7	10	8	9	8	9	10*10=100	100*7=700
	[A]Difusión de Software Dañino.	7	8	10	9	9	8	10 * 10 = 100	100*7=700
	[I] Fallo de servicio de comunicaciones.	3	5	10	4	4	5	10*10=100	100*3=300
Impresoras	[E] Errores de mantenimiento y actualización de Hardware.	3	5	9	6	7	8	9 * 9 = 81	81* 3 = 243
	[I] Avería de origen Físico o lógico.	5	4	10	7	5	6	9 * 10 = 90	90 * 5 =450
	[A] Daño por manipulación de funcionarios.	4	3	10	5	6	5	9 * 10 = 90	90 * 4= 360
	[I]Condiciones inadecuadas de temperatura y/o humedad.	2	2	3	3	4	3	9 * 8 = 64	64 * 2= 128
	[I] Contaminación Medioambiental.	3	2	5	3	5	6	9 * 10 = 90	90 * 3 = 270
	[A] Acceso no autorizados.	2	4	3	4	4	3	9 * 8 = 72	72 * 2 = 144
	[A] Uso no previsto.	5	3	3	2	5	6	9 * 10 = 90	90 * 5 = 450
	[N] Desastres naturales.	3	5	10	7	5	7	9 * 10 = 90	90* 3= 270
	[N] Fuego.	1	4	10	7	6	6	9 * 10 = 90	90 * 1 = 90
	[N] Daños por agua.	3	4	10	7	8	8	9 * 10 = 90	90* 3 = 270
	[I] Corte del suministro eléctrico.	4	3	10	8	7	6	9 * 10 = 90	90*4=360
	[A] Abuso de privilegios de acceso.	4	7	8	6	7	8	9 * 10 = 90	90*4=360
	[I] Fallo de servicio de	2	5	10	4	6	5	9 * 10 = 90	90*2=180

	comunicaciones.								
	[E] Errores de Administrador.	3	7	10	4	6	7	9 * 10 = 90	90*3=270
	[A]Robo de hardware	1	8	10	6	5	6	9 * 9 = 81	81*1=81
Escáner	[E] Errores de mantenimiento y actualización de Hardware.	3	4	9	5	7	8	6 * 9 = 54	54 * 3 = 162
	[A] Uso no previsto.	5	4	3	3	4	5	6 * 8 = 48	48* 5 = 240
	[A] Acceso no autorizados.	4	5	5	6	6	4	6 * 8 = 48	48 * 4 =192
	[I] Avería de origen Físico o lógico.	3	4	10	7	8	6	6 * 10 =60	60 * 3 =180
	[A] Daño por manipulación de funcionarios.	2	2	10	9	6	8	6 * 10 = 60	60 * 2 = 120
	[I] Contaminación Medioambiental.	5	1	8	2	2	3	6 * 8 = 48	48 * 5 = 240
	[N] Fuego.	1	2	10	2	3	2	6 * 10 = 60	60 * 1 = 60
	[N] Desastres naturales.	3	2	10	2	7	8	6 *10 = 60	60 * 3 = 180
	[I] Corte del suministro eléctrico	4	2	10	2	3	2	6*10 = 60	60 * 4 = 240
	[I]Condiciones inadecuadas de temperatura y/o humedad.	3	2	8	4	3	3	6 * 7 = 42	42 * 3= 126
	[A] [Robo]	1	8	10	6	5	6	6*9= 54	54 * 1 = 54
	[A] Abuso de privilegios de acceso.	3	3	8	4	3	4	6 * 8 = 48	48 * 3 = 144
	[E] Errores de Administrador.	2	7	10	6	5	6	6*10=60	60 * 2 = 120
	[N] Daños por agua	3	4	10	4	3	3	6*10=60	60 * 3 = 180
	[A] Daño por manipulación de funcionarios.	3	2	10	9	6	8	8 * 10 = 80	80*3=240
	[N] Desastres naturales.	3	2	10	2	7	8	8 *10 =80	80 *3 = 240

Telefonía IP	[A] Acceso no autorizados.	3	5	5	6	6	4	8*8=64	64*3= 192
	[I] Contaminación Medioambiental.	5	1	8	2	2	3	8 *5 = 40	40 *5 =200
	[I] Fallo de servicio de comunicaciones.	3	5	10	4	5	4	8*8=64	64*3=192
	[A] Abuso de privilegios de acceso.	3	3	8	4	3	4	8*9=72	72*3=216
	[I] Avería de origen Físico o lógico.	3	8	10	7	8	9	8 * 8 =64	64*3 = 192
	[E] Errores de Administrador.	2	7	10	6	5	6	8 * 9 = 72	72*2 = 144
	[A] Uso no previsto.	4	4	3	3	4	5	8 * 7 = 56	56 * 4 = 244
	[N] Daños por agua	3	4	10	4	3	3	8*8 =64	64* 3=192
	[N] Fuego.	1	2	10	2	3	2	8 * 10 = 80	80 * 1 = 80
UPS	[I] Avería de origen Físico o lógico.	4	3	10	3	4	4	10* 10 = 100	100* 4 = 400
	[I] Contaminación Medioambiental.	3	6	9	8	7	8	10 * 9 = 90	90* 3 = 270
	[N] Daños por agua	2	8	10	7	6	7	10 * 10 = 100	100* 2 = 200
	[N] Desastres naturales.	3	8	10	8	9	8	10 * 10 = 100	100* 3 = 300
	[I]Condiciones inadecuadas de temperatura y/o humedad.	3	4	10	7	5	7	10 * 10 = 100	100* 4= 300
	[N] Fuego.	1	9	10	9	9	9	10 * 10 = 100	100*1=100
	[I] Corte del suministro eléctrico.	3	9	10	7	8	8	10 * 10 = 100	100*3=300
	[E] Errores de Administrador.	2	8	10	6	9	8	10*10=100	100*2=200
SOFTWARE									
Sistema Operativo	[A] Difusión de software dañino.	6	9	10	8	8	8	9 * 10 = 90	90*6=630
	[A]Acceso no autorizado.	4	8	9	8	9	8	9 * 9 = 81	81*4=324
	[I] Avería de origen Físico o lógico.	3	5	10	5	3	4	9 * 9 = 81	81 * 3 = 243
	[E] Errores mantenimiento y actualización de software.	4	9	10	9	7	8	9 * 10 = 90	90 * 4 = 360
	[A] Suplantación de la identidad del usuario.	5	10	9	10	10	8	9 * 10 = 900	90*4= 450
	[A] Abuso de privilegios de acceso.	5	9	8	9	9	8	9 * 8 = 72	72 * 5= 360
	[A] Daño por manipulación de	4	7	10	8	5	4	9 * 9 = 81	81 * 4= 324

	funcionarios.								
	[E] Errores de los usuarios.	3	9	10	9	7	8	9 * 10 = 90	90 * 3 = 270
	[E] Errores de Administrador.	2	9	10	9	7	8	9 * 10 = 90	90 * 2 = 180
Aplicativo Web.	[A] Suplantación de la identidad del usuario.	3	10	9	9	10	9	10 * 10 = 100	100*3=300
	[E] Errores mantenimiento y actualización de software.	3	7	10	8	9	8	10*10= 100	100 * 3 = 300
	[I] Fallo de servicio de comunicaciones.	3	2	10	5	4	5	10*10=100	100*3=300
	[A] Daño por manipulación de funcionarios.	2	7	10	8	4	4	10*10=100	100*2=200
	[E] Errores de los usuarios.	3	10	10	10	9	9	10 * 10 = 100	100*3 = 300
	[A] Acceso no autorizado.	3	9	8	9	9	9	10 * 10 = 100	100*3=300
	[A]Eliminación de la información.	2	9	10	9	8	8	10*10=100	100*2=200
	[A] Divulgación de la información.	7	10	9	9	8	9	10*10=100	100*7=700
	[I] Avería de origen Físico o lógico.	3	8	10	10	8	7	10 * 10 = 100	100 * 3 = 300
	[A] Modificación de la información.	4	9	10	10	10	9	10 * 10 = 100	100*4=400
	[E] Alteración accidental de la información.	6	8	10	10	10	5	10 * 10 = 100	100*6=600
	[I]Caída del sistema por agotamiento de recursos.	5	8	10	7	4	5	10 * 10 = 100	100*5=500
	[A] Abuso de privilegios de acceso.	5	9	9	8	10	8	10 * 10 = 100	100*5=500
	Denegación de servicio.	2	8	10	7	8	8	10 * 10 = 100	100*2=200
Antivirus	[E] Errores mantenimiento y actualización de software.	2	6	10	7	6	5	9 * 10 = 90	90 * 2 = 180
	[E] Errores de Administrador.	2	5	10	4	8	7	9*10=90	90*2=180
	[I] Avería de origen Físico o lógico.	4	7	9	7	6	4	9 * 6 = 54	54 * 4 = 216

Navegadores Web	A] Suplantación de la identidad del usuario.	5	10	9	10	10	8	9 * 10 = 90	90 * 5 =450
	[A] uso no previsto.	5	9	4	5	7	6	9 * 10 = 90	90 * 5 = 450
	[E]Caída del sistema por agotamiento de recursos.	3	6	10	7	8	9	9 * 10 =90	90 * 3 = 270
	[A] Daño por manipulación de funcionarios.	2	5	6	7	4	5	9 * 10 =90	90 * 2 =180
	[A] Abuso de privilegios de acceso.	3	8	9	8	7	8	9 * 9 = 81	81 * 3 = 243
	[E] Errores mantenimiento y actualización de software.	2	7	10	8	6	7	9 * 8 = 72	72 * 2 = 144
	[E] Errores de los usuarios.	5	7	8	9	8	7	9 * 9 = 81	81 * 5 = 405
	[A] Acceso no autorizado.	4	10	9	10	9	10	9 * 10= 90	90 * 4 = 360
	[I] Avería de origen Físico o lógico.	2	9	10	9	7	9	9 * 10 = 90	90 * 2 = 180
Correo electrónico.	[A] Suplantación de la identidad del usuario.	5	10	10	9	9	9	10 * 10 =100	100 * 5 =500
	[E] Errores de mantenimiento o actualización de software.	3	5	10	8	9	8	10 * 10= 100	100 * 3 =300
	[I] Avería de origen Físico o lógico.	2	8	10	7	8	7	10 * 10 =100	100 * 2 = 200
	[A] Acceso no autorizado.	4	9	6	8	9	9	10 * 10 =100	100 * 4 =400
	[E]Caída del sistema por agotamiento de recursos.	3	7	10	6	9	8	10 * 10 =100	100 * 3 = 300
	[E] Errores de Administrador.	2	7	10	6	4	6	10 * 10= 100	100 * 2 =200
	[E] Errores de los usuarios.	3	9	10	10	10	9	10 * 10 =100	100 * 3 =300
	[A]Denegación de servicio.	2	8	10	9	8	4	10 * 10 =100	100 * 2 =200
	[E]Difusión de software dañino.	2	8	9	5	7	5	10 * 9 = 90	90 * 2=180
	[A] Uso no previsto.	5	4	5	6	8	7	10 * 10= 100	100*5=500
	[I] Fallo de servicio de comunicaciones.	2	4	10	3	4	5	10*10=100	100*2=200

	[A] Daño por manipulación de funcionarios.	2	8	10	7	4	6	10*10=100	100*2=200
	[A] Abuso de privilegios de acceso.	4	7	4	8	9	6	10 * 10= 100	100 * 4 =400
ARCHIVOS FISICOS									
Documentos Físicos.	[E] Alteración accidental de la información.	5	8	10	10	9	5	10 * 10= 100	100*5=500
	[A] Eliminación de Información.	3	10	10	9	9	10	10 * 10= 100	100*3=300
	[A] Modificación de la información	4	9	10	10	9	8	10 * 10= 100	100*4=400
	[E] Errores de los usuarios.	5	10	9	10	9	10	10*10=100	100*5=500
	N] Daños por desastres naturales.	3	7	10	8	6	4	10 * 10= 100	100*3=300
	[A] Divulgación de información.	5	10	9	8	8	4	10 * 10= 100	100*5=500
	[N] Fuego.	1	10	10	10	10	3	10 * 10= 100	100*1=100
	[A] perdida de documentos	8	10	10	10	7	6	10 * 10= 100	100*8=800
	[N]Daños por agua	3	8	10	9	6	5	10 * 10 =100	100*3=300
	[N] Desastres naturales.	3	8	10	9	5	4	10 * 10=100	100*3=300
ARCHIVOS DIGITALES									
Información Digital del PC	A] modificación de la Información.	5	9	10	10	9	8	10 * 10= 100	100*5=500
	[I]Avería de origen Físico o lógico.	2	8	10	8	3	4	10 * 9=90	90 * 2 = 180
	[E]Difusión de software dañino	3	5	10	7	5	6	10*10=100	100*3=300
	[A]Perdida de información	7	7	10	10	5	5	10*10=100	100*7=700
	[N] Daños por desastres naturales.	3	6	10	7	5	4	10*10=100	100*3=300
	[A] Divulgación de Información.	5	10	8	8	8	9	10 * 10= 100	100*5=500
	[A] Abuso de privilegios de acceso.	7	9	8	9	10	9	10 * 10= 100	100*7=700

	Eliminación de la información.	5	8	10	10	9	8	10 * 10= 100	100*5=500
	[E] Errores de los usuarios.	6	9	10	10	8	9	10 * 10= 100	100*6=600
	[E] Alteración accidental de la información.	5	8	10	10	8	7	10 * 10= 100	100*5=500
	[A] Suplantación de la identidad del usuario.	5	10	8	9	8	8	10 * 10= 100	100*5=500
RECURSOS HUMANO									
Personal.	[A] Ingeniería Social-	5	10	10	10	9	9	9 * 10 = 90	90 * 5 = 450
	[A] Indisponibilidad del personal.	2	8	10	9	10	9	9*10=90	90 * 2 =180

Fuente: El autor.

9.5 NIVEL DE LOS RIESGOS

Teniendo en cuenta los resultados de la gráfica anterior, se clasifican los riesgos de acuerdo a su nivel:

Tabla 18: Niveles de Riesgos

NIVEL DE RIESGO				
BAJO >10 y ≤200	**MEDIO >200 y ≤400**	**ALTO >400 y ≤ 600**	**MUY ALTO >600 y ≤ 800**	**CRITICO >800**

Fuente: El autor.

Tabla 19: Nivel de Riesgo

CLASIFICACIÓN	ACTIVOS	Bajo	Medio	Alto	Muy Alto	Critico
COMUNICACIONES RACK	[N] Daños por agua.					
	[N] Desastres naturales.					
	[I] Condiciones inadecuadas de temperatura y/o humedad.					
	[I] Contaminación Medioambiental.					
	[N] Fuego					
	[I] Avería de origen Físico o lógico					
	[A] Abuso de privilegios de acceso.					
	[A] Acceso no autorizados.					
SWITCH	[N] Fuego.					
	[N] Daños por agua.					
	[N] Desastres naturales.					
	[I] Condiciones inadecuadas de temperatura y/o humedad.					
	[I] Contaminación Medioambiental.					
	[I] Avería de origen Físico o lógico.					
	[A] Acceso no autorizados.					
	[I]Caída del sistema por agotamiento de recursos.					
	[I] Denegación del servicio.					
	[I] Corte del suministro eléctrico.					
	[I]Fallo de servicio de comunicaciones.					

	[E] Errores de Administrador.					
	[A] Robo.					
	[A] Abuso de privilegios de acceso.					
	[I] Denegación del servicio.					
	[N] Daños por agua.					
	[N] Desastres naturales.					
	[I] Condiciones inadecuadas de temperatura y/o humedad.					
	[I] Contaminación Medioambiental.					
	[A]Robo.					
	[I] Avería de origen Físico o lógico					
	[N] Fuego.					
	[A] Acceso no autorizados.					
	[I] Corte del suministro eléctrico					
	[I]Caída del sistema por agotamiento de recursos.					
	[I] Fallo de servicio de comunicaciones.					
	[E] Errores de Administrador.					
	[A] Abuso de privilegios de acceso.					
COMPUTADORES						
	[A] Robo de hardware.					
	[N] Daños por agua.					
	[N] Desastres naturales.					
	[I]Condiciones inadecuadas de temperatura y/o humedad.					
	[I] Contaminación Medioambiental.					
	[A] Modificación de la información					
	[A]Suplantación de la identidad del usuario.					
	[I] Avería de origen Físico o lógico.					
	[N] Fuego.					
	[E] Errores de mantenimiento y actualización de Hardware.					
	[A] Acceso no autorizados.					
	[A] Uso no previsto.					
	[I] Corte del suministro eléctrico.					
	[E] Errores de Administrador.					
	[A] Daño por manipulación de usuarios.					
	[A] Abuso de privilegios de acceso.					
	[A] Divulgación de la información.					
	[A]Difusión de Software Dañino.					
	[I] Fallo de servicio de comunicaciones.					

HARDWARE						
IMPRESORAS	[E] Errores de mantenimiento y actualización de Hardware.					
	[I] Avería de origen Físico o lógico.					
	[A] Daño por manipulación de funcionarios.					
	[I]Condiciones inadecuadas de temperatura y/o humedad.					
	[I] Contaminación Medioambiental.					
	[A] Acceso no autorizados.					
	[A] Uso no previsto.					
	[N] Desastres naturales.					
	[N] Fuego.					
	[N] Daños por agua.					
	[I] Corte del suministro eléctrico.					
	[A] Abuso de privilegios de acceso.					
	[I] Fallo de servicio de comunicaciones.					
	[E] Errores de Administrador.					
	[A]Robo de hardware					
ESCÁNER						
	[E] Errores de mantenimiento y actualización de Hardware.					
	[A] Uso no previsto.					
	[A] Acceso no autorizados.					
	[I] Avería de origen Físico o lógico.					
	[A] Daño por manipulación de funcionarios.					
	[I] Contaminación Medioambiental.					
	[N] Fuego.					
	[N] Desastres naturales.					
	[I] Corte del suministro eléctrico					
	[I]Condiciones inadecuadas de temperatura y/o humedad.					
	[A] [Robo]					
	[A] Abuso de privilegios de acceso.					
	[E] Errores de Administrador.					
	[N] Daños por agua					
	[A] Daño por manipulación de funcionarios.					
	[N] Desastres naturales.					
	[A] Acceso no autorizados.					
	[I] Contaminación Medioambiental.					

TELEFONÍA IP	[I] Fallo de servicio de comunicaciones.					
	[A] Abuso de privilegios de acceso.					
	[I] Avería de origen Físico o lógico.					
	[E] Errores de Administrador.					
	[A] Uso no previsto.					
	[N] Daños por agua					
	[N] Fuego.					
UPS						
	[I] Avería de origen Físico o lógico.					
	[I] Contaminación Medioambiental.					
	[N] Daños por agua					
	[N] Desastres naturales.					
	[I]Condiciones inadecuadas de temperatura y/o humedad.					
	[N] Fuego.					
	[I] Corte del suministro eléctrico.					
	[E] Errores de Administrador.					
SOFTWARE						
SISTEMA OPERATIVO	[A] Difusión de software dañino.					
	[A]Acceso no autorizado.					
	[I] Avería de origen Físico o lógico.					
	[E] Errores mantenimiento y actualización de software.					
	[A] Suplantación de la identidad del usuario.					
	[A] Abuso de privilegios de acceso.					
	[A] Daño por manipulación de funcionarios.					
	[E] Errores de los usuarios.					
	[E] Errores de Administrador.					
APLICATIVO WEB						
	[A] Suplantación de la identidad del usuario.					
	[E] Errores mantenimiento y actualización de software.					
	[I] Fallo de servicio de comunicaciones.					
	[A] Daño por manipulación de funcionarios.					
	[E] Errores de los usuarios.					
	[A] Acceso no autorizado.					
	[A]Eliminación de la información.					
	[A] Divulgación de la información.					

	[I] Avería de origen Físico o lógico.					
	[A] Modificación de la información.					
	[E] Alteración accidental de la información.					
	[I]Caída del sistema por agotamiento de recursos.					
	[A] Abuso de privilegios de acceso.					
	Denegación de servicio.					
ANTIVIRUS						
	[E] Errores mantenimiento y actualización de software.					
	[E] Errores de Administrador.					
	[I] Avería de origen Físico o lógico.					
NAVEGADOR WEB						
	A] Suplantación de la identidad del usuario.					
	[A] uso no previsto.					
	[E]Caída del sistema por agotamiento de recursos.					
	[A] Daño por manipulación de funcionarios.					
	[A] Abuso de privilegios de acceso.					
	[E] Errores mantenimiento y actualización de software.					
	[E] Errores de los usuarios.					
	[A] Acceso no autorizado.					
	[I] Avería de origen Físico o lógico.					
CORREO ELECTRÓNICO						
	[A] Suplantación de la identidad del usuario.					
	[E] Errores de mantenimiento o actualización de software.					
	[I] Avería de origen Físico o lógico.					
	[A] Acceso no autorizado.					
	[E]Caída del sistema por agotamiento de recursos.					
	[E] Errores de Administrador.					
	[E] Errores de los usuarios.					
	[A]Denegación de servicio.					
	[E]Difusión de software dañino.					
	[A] Uso no previsto.					
	[I] Fallo de servicio de comunicaciones.					
	[A] Daño por manipulación de funcionarios.					
	[A] Abuso de privilegios de acceso.					

DOCUMENTOS FISICOS						
	[E] Alteración accidental de la información.					
	[A] Eliminación de Información.					
	[A] Modificación de la información					
	[E] Errores de los usuarios.					
	N] Daños por desastres naturales.					
	[A] Divulgación de información.					
	[N] Fuego.					
	[A] perdida de documentos					
	[N]Daños por agua					
	[N] Desastres naturales.					
INFORMACIÓN DIGITAL						
	A] modificación de la Información.					
	[I]Avería de origen Físico o lógico.					
	[E]Difusión de software dañino					
	[A]Perdida de información					
	[N] Daños por desastres naturales.					
	[A] Divulgación de Información.					
	[A] Abuso de privilegios de acceso.					
	Eliminación de la información.					
	[E] Errores de los usuarios.					
	[E] Alteración accidental de la información.					
	[A] Suplantación de la identidad del usuario.					
	[A] Ingeniería Social-					
	[A] Indisponibilidad del personal.					

Fuente: El autor.

9.6 TRATAMIENTO DE LOS RIESGOS.

Una vez que se conocen los riesgos de la organización, se procede a realizar su tratamiento de acuerdo a las acciones a tomar sobre cada uno, se tienen en cuenta los siguientes parámetros.[12]

- Mitigar el riesgo: Se trata de reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable.

- Asumir el riesgo: La Dirección asume el riesgo ya que está por debajo de un valor de riesgo aceptable.

- Transferir el riesgo a un tercero: Se trata de subcontratar un tercero para que se encargue de tomar medidas para mitigar ese riesgo.

- Eliminar el riesgo: Esta opción es complicada porque los riesgos siempre están presentes, al menos que elimine el activo, el proceso o área del negocio.

Para realizar el tratamiento de riesgos, se seleccionaron los riesgos de mayor impacto de acuerdo a los resultados de la tabla anterior, los Altos, Muy altos y Críticos.

[12] Ing. José Manuel Poveda, Análisis y Valoración de los Riesgos, Modulo 8, ISO 27001. Tomado el día 30 de Julio del 2015. [En línea]. https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

Tabla 20: Tratamiento de los Riesgos.

Categorías	Riesgos	Impacto	Tratamiento del Riesgo	Área Afectada
Información.	Pérdida de documentos.	Crítica	Mitigar: Controles en toda la organización. 1. hacer regularmente Backup de toda la información esencial del negocio. 2. aplicar control en las oficinas, despachos y recursos. 3. controles de entrada que garanticen el acceso únicamente por personal autorizado. 4. Capacitar a personal sobre la manipulación de los documentos. 5. Instalar software que permita bloquear los puertos USB. 6. Se debe instalar herramientas para la prevención de fuga de Información.	Funcionarios, procesos
	Modificación de información Alteración accidental de la información. Perdida de información	Alta Alta Muy alta.	Mitigar: Controles en toda la organización. 1. Sensibilizar a los funcionarios sobre las buenas prácticas de políticas de seguridad, uso de contraseñas, bloqueo de sesión, entre otras. 2. Restringir y controlar la asignación y uso de los privilegios. 3. Se retiran los archivos cuando el computador cambia de usuario. 4. Se debe desarrollar e implantar una política de uso de controles criptográficos para la protección de la información.	Funcionarios, procesos

	Divulgación de información	Alta	Mitigar: Controles en toda la organización. 1. Sensibilizar a los funcionarios sobre las buenas prácticas de políticas de seguridad, uso de contraseñas, bloqueo de sesión, entre otras. 2. Establecer acuerdos de confidencialidad en contratación de personal. 3. se retiran los archivos cuando el computador cambia de usuario 4. Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o Uso no autorizados o inadecuado. 5. Cuando se le da de baja a un equipo se debe formatear todo el equipo	Funcionarios, empresa.
Hardware	Daños por manipulación de usuarios. Errores de los usuarios.	Alto	Mitigar: Realizar capacitaciones a los usuarios sobre el uso de los recursos informáticos. 1. Establecer términos y condiciones de responsabilidad en la contratación de personal. 2. Concienciación, formación y capacitación en seguridad informática y uso de los recursos informáticos, manejo de aplicaciones instituciones.	LAN – Equipos, usuarios, hardware y software.
	Uso no previsto	Alto	Mitigar: Concientizar al personal que los recursos tecnológicos son de uso exclusivo para actividades laborales. 1. Los empleados y contratistas deben recibir capacitación apropiada sobre las políticas y procedimientos de la organización así como el buen uso de los recursos informáticos. 2. Se deben establecer e indicar a los funcionarios las	Hardware y software.

			condiciones de uso de los recursos informáticos manteniendo su disponibilidad e integridad. 3.	
	Suplantación de la identidad del usuario.	Alto	Mitigar: Identificación y Autenticación de usuario. 1. Los sistemas de gestión de contraseñas deberían ser iterativos y garantizar la calidad de las contraseñas. 2. Política para escritorios y monitores limpios de información. 3. Concienciación, formación y capacitación en seguridad informática y uso de los recursos informáticos.	Usuarios, imagen de la empresa, archivos digitales.
Software	Acceso no autorizado.	Alto	Mitigar: Política de Control de acceso a la red y a las aplicaciones. 1. Se debe proveer a los usuarios de los accesos a los servicios para los que han sido expresamente autorizados a utilizar. 2. Se deben controlar la configuración y el acceso físico y lógico a los puertos de diagnóstico. 3. El departamento de sistemas actualiza los permisos de acceso cuando se entera del retiro de un funcionario.	Funcionarios, procesos, software.
	Caída del sistema por agotamiento de recursos	Alto	Mitigar: monitorear el ancho de banda de la red, para evitar congestión. 1. Ampliar el ancho de banda del internet. 2. Deberían mantener y controlar adecuadamente la red para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones.	LAN, usuarios y aplicativos web.
	Abuso de privilegios de acceso.	Muy Alto	Mitigar: monitorear la plataforma tecnológica y el acceso a las aplicaciones. 1. Se deben restringir y asignar el uso de privilegios. 2. Contar con un software de seguridad que bloquee los accesos no autorizados en la red. 3. Controlar el acceso al sistema operativo mediante procedimientos seguros de conexión.	Funcionarios, software, red.
	Avería de origen Físico o lógico.	Alto	Mitigar: Programar mantenimientos preventivos a software y hardware.	

			1. Se deben mantener continuamente los equipos para garantizar su continua disponibilidad e integridad. 2. Programar mantenimientos preventivos.	Funcionarios, servicios.
	Difusión de software dañino.	Crítico	Mitigar: Implementar métodos o herramientas de protección contra software dañino. 1. instalación de antimalware. 2. actualización de antivirus. 3. escaneo de memoria USB. 4. Actualizar el sistema operativo. 5. Instalar software que permita bloquear los puertos USB. .	LAN – Internet, Computadores, usuarios internos,
Recurso Humano	Ingeniería Social-	Alta	Mitigar: Enseñarle a los usuarios sobre las técnicas y estrategias que existen para el robo de contraseñas y suplantar a la persona. . 1. Se debería restringir y controlar la asignación y uso de los privilegios. 2.	Procesos.

Fuente: El autor

9.7 OBJETIVOS DE CONTROL.

Se aplican para mitigar o reducir el riesgo hasta unos niveles asumibles por la organización, los controles deben producir reducción en la degradación y frecuencia de la amenaza para cada dimensión.

La aplicación de controles se realizó, apoyada en la norma ISO 27002.

Tabla 21: Asignación de controles a cada riesgo.

RIESGOS	OBJETIVOS DE CONTROL	CONTROLES.	DEFINICION DEL CONTROL
Eliminación de información;	10.5 Copias de seguridad.	10.5.1 Copias de seguridad de la información.	Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software.
Modificación de información.	11.2 Gestión de acceso de usuario.	11.2.1 Registro de usuario.	Existir un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información.
		11.2.2 Gestión de privilegios.	Restringir y controlar la asignación y uso de los privilegios.
Acceso no autorizado.		11.2.3 Gestión de contraseñas.	Controlar la asignación de contraseñas mediante un proceso de gestión formal.
Divulgación de información.	11.3 Responsabilidades de usuario.	11.3.1 Uso de contraseñas.	Exigir a los usuarios el uso de las buenas prácticas de seguridad en la selección y uso de las contraseñas.
		11.3.2 Equipo de usuario desatendido.	Sensibilizar a los funcionarios para bloquear el equipo en periodo de inactividad.
Alteración accidental de la información.		11.3.3 Política de puesto de trabajo desatendido y pantalla limpia.	Política para escritorios y monitores limpios de información.
		11.5.1 Procedimiento seguro de inicio de sesión.	Deben controlar el acceso al sistema operativo mediante procedimientos seguros de conexión.

Suplantación de identidad de usuario.	11.5 Control de acceso al sistema operativo.	11.5.2 Identificación y Autenticación de usuario.	Todos los usuarios deben disponer de un único identificador propio personal, mediante técnicas de autenticación.
		11.5.3 sistema de gestión de contraseñas.	Los sistemas de gestión de contraseñas deberían ser iterativos y garantizar la calidad de las contraseñas.
		11.5.4 uso de los recursos del sistema.	Restringir y controlar muy de cerca el uso de programas de utilidad del sistema que pudieran ser capaces de eludir los controles.
		11.5.5Desconexión automática de sesión.	Se debe cerrar la sesión tras un periodo de inactividad.
Abuso de privilegios de acceso.	11.4 Control de acceso a la red.	11.4.1 Política de uso de los servicios en red.	Se debe proveer a los usuarios de los accesos a los servicios para los que han sido expresamente autorizados a utilizar.
		11.4.2 Autenticación de usuario para conexiones externas.	Se deben utilizar métodos de autenticación adecuados para el control del acceso remoto de los usuarios.
		11.4.3 Identificación de los equipos en la red.	Se deben considerar la identificación automática de los equipos como un medio de autenticación de conexiones.
		11.4.4 Protección de los puertos de diagnóstico y configuración remotos.	Se deben controlar la configuración y el acceso físico y lógico a los puertos de diagnostico.
		11.4.6 Control de la conexión a la red.	Se deben restringir las competencias de los usuarios para conectarse en red según la política de control de acceso y necesidad de uso de las aplicaciones.

Difusión de software dañino.	10.4 Protección contra el código malicioso y descargable.	10.4.1 Controles contra el código malicioso.	Se deben implantar controles de detección, prevención, y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de usuarios.
		10.4.2 Controles contra el código descargado en el cliente.	Se debe asegurar que el código móvil opera de acuerdo a una política de seguridad definida y se debería evitar la ejecución de los códigos no autorizados.
Avería de origen físico y lógico. Robo o Pérdida de documentos físicos	9.1 Áreas seguras.	9.1.1 Perímetro de seguridad física.	Los perímetros como paredes, puertas, puesto de recepción deben utilizarse para proteger las áreas que contengan información y recurso para su procesamiento.
		9.1.2 Controles físicos de entrada.	Deben estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente por personal autorizado.
		9.1.3 Seguridad de oficinas, despachos e instalaciones.	Se debe aplicar control en las oficinas, despachos y recursos.
		9.1.4 Protección contra las amenazas externas y de origen ambiental.	Se deben aplicar medidas de protección física contra incendio, terremoto, inundación, explosión u otro desastre natural.
		9.1.5 Trabajo en área segura.	Se debe controlar las áreas de carga y descarga con objeto de evitar accesos no autorizados.
	14.1 Gestión de la continuidad del negocio.	14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	Se debe desarrollar y mantener un proceso de gestión de la continuidad del negocio, que trate los requerimientos de seguridad de la información necesarios para la continuidad.
		. 14.1.2 Continuidad del negocio y evaluación de	Se deben identificar los eventos que puedan causar interrupciones a los procesos de negocio

		riesgos	junto con la probabilidad e impacto de dichas interrupciones y consecuencias para la seguridad de información.
		14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información	Se debe desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información, tras una interrupción o fallo de los procesos críticos del negocio.
		14.1.5Pruebas, mantenimiento y reevaluación de planes de continuidad.	Se deben probar regularmente los planes de continuidad del negocio para garantizar su actualización y eficacia.
	10.7 Manipulación de los soportes.	10.7.1 Gestión de soporte extraíbles.	Se deben establecer procedimientos para la gestión de los medios informáticos removibles.
		10.7.4 Seguridad de la documentación del sistema.	Se deben proteger la documentación de los sistemas contra acceso no autorizados.
Daños por manipulación de usuarios. Errores de los usuarios. Ingeniería social. Uso no previsto.	8.1 Antes del empleo.	8.1.1 Funciones y responsabilidades.	Se deben definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas en concordancia con la política de seguridad de la información.
		8.1.3 Términos y condiciones de contratación.	Los empleados, contratistas y terceros deberían aceptar y confirmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones de la organización para la seguridad de información.
	8.2 Durante el empleo.	8.2.2 Concienciación, formación y capacitación en seguridad informática.	Los empleados y contratistas deben recibir capacitación apropiada sobre las políticas y procedimientos de la organización como son relevantes para la función de su trabajo.
	8.3 Cambio del puesto	8.2.3 Proceso disciplinario.	Debe existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad.

	trabajo	8.3.1 Responsabilidad al cambio.	La responsabilidad para ejecutar la finalización de un empleo o el cambio de este deberían estar claramente definidas y asignadas.
		8.3.2 Devolución de activos.	Todos los empleados y contratistas deberían devolver los activos asignados en su posesión a la finalización de su contrato.
		8.3.3 Retirada de los derechos de acceso.	Deberían retirar los derechos de acceso para todos los empleados, contratistas y a las instalaciones del procesamiento de información a la finalización del empleo o contrato.
Caída por agotamiento del sistema.	10.6 Gestión de seguridad en las redes. 13.1 notificación de eventos y puntos débiles de la seguridad	10.6.1 controles de red. 10.6.2 seguridad de los servicios de red.	Deberían mantener y controlar adecuadamente la red para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones.

Fuente: el autor

10. POLITICAS DE SEGURIDAD.

Este documento describe las políticas y normas de seguridad de la información definidas por el ICBF, Centro Zonal Virgen y Turístico, Regional Bolívar. Para la elaboración del mismo, se tomaron como referencia la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.

Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información y se convierten en la base para la Implantación de los controles, procedimientos y estándares. La política de seguridad completa se puede detallar en el anexo A.

11. PROCEDIMIENTOS DOCUMENTADOS

Los procedimientos documentados son de gran ayuda en el diseño del sistema de gestión de seguridad de la información, en el presente documento se explican los procedimientos de gestión de incidentes, procedimientos tecnológicos y procedimiento de continuidad del negocio.

11.1 PROCEDIMIENTOS TECNOLOGICOS

Dentro del listado de procedimientos tecnológicos que existen en una empresa, solo se contemplaron los siguientes: Procedimientos de Backup, Procedimiento de solicitud de correo institucional, Procedimiento para solicitud de soporte técnico, Procedimiento de solicitud de acceso a equipos informáticos. Estos procedimientos vienen debidamente documentados en el anexo B de este documento.

11.2 PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES.

Este tipo de procedimiento, son una guía para responder en forma adecuada a la ocurrencia de incidentes de seguridad informática que afecten real o potencialmente sus servicios, los procedimientos de gestión de incidentes se encuentran definidos en detalle en el anexo B.

.

11.3 PLAN DE CONTINUIDAD DEL NEGOCIO.

Este documento está diseñado para permitir la continuidad de las operaciones una vez ha ocurrido un incidente de seguridad de la información. El plan completo se encuentra descrito en el anexo B.

12. COSTO DEL PROYECTO

El costo del proyecto se tiene en cuenta el tiempo invertido el valor hora de trabajo, los gastos de trasporte, papelería invertida más los imprevistos.

Tabla 22: Presupuesto del Proyecto

	ITEM	**VALOR**
1	Equipos (computador, impresora, escáner).	$ 200.000
2	Valor Horas de trabajo Una hora: 12.500 4 horas a la semana: 50.000 * los 6 meses de ejecución del proyecto.	$ 1.200.000
2	Transporte y visitas de campo.	$ 300.000
3	Papelería y fotocopias	$ 300.000
4	Impresión	$ 300.000
5	Servicio de Internet.	$ 150.000
6	Varios e Imprevistos	$ 500.000
	TOTAL	$ 2.950.000

Fuente: El Autor.

13. RECURSOS DEL PROYECTO

Para el desarrollo de este proyecto se tienen en cuenta recursos humanos, físicos y tecnológicos. A continuación se describe cada uno de los recursos necesarios en el desarrollo del proyecto:

- Recurso Humano: los usuarios internos del centro zonal la Virgen ICBF regional Bolívar.

- Recurso Físico: Recursos Tecnológicos, Infraestructura física, puestos de trabajo, Documentación física y digital.

- Recursos Tecnológicos: Computador, Impresoras, Escáner.

14. CRONOGRAMA DEL PROYECTO

Tabla 23: Cronograma de Actividades..

ITEM	ACTIVIDADES	MES 1	MES 2		
	PLANEAR				
1	Analizar el flujo de información misional y crítica de la empresa.				
2	Definir el alcance los límites del SGSI teniendo en cuenta los activos de información, sistemas de información y los recursos tecnológicos				
3	Establecer la política de seguridad de la empresa.				
4	Identificar los activos y sus propietarios tales como la información, software, hardware infraestructura, recursos tecnológicos y recurso humano				
5	Identificar las amenazas que afectan los activos				
6	Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas.				
7	Identificar los impactos que puedan tener la perdida de confidencialidad, disponibilidad e integridad de la información				
8	Realizar el análisis y evaluación de los riesgos de los activos de información				
9	Identificar una metodología para realizar la valoración de los riesgos.				
10	Identificar los riesgos que afectan los activos.				
11	Diseñar un plan para mitigar los riesgos				
12	Mencionar los controles a implementar para minimizar los riesgos.				

Fuente: El autor.

15. CONCLUSIONES

El presente proyecto cumplió todos los objetivos y se logró diseñar el sistema de gestión de seguridad de la información para el ICBF, Centro Zonal Virgen y Turístico, Regional Bolívar. Al finalizar el presente proyecto se obtuvieron las siguientes conclusiones:

- Se identificaron los activos de información con su respectivo inventario.

- Se identificaron todas las vulnerabilidades y amenazas en la empresa, realizando un listado con su respectiva valoración del estado actual de los activos.

- Se realizó la gestión de riesgos utilizando la metodología MAGERIT, identificando los riesgos de mayor afectación para la empresa de acuerdo a los resultados del nivel de valoración.

- Se identificaron los riesgos altos, muy altos y críticos y se realizó el tratamiento adecuado para cada uno de ellos.

- Se establecieron los objetivos de control y controles para cada riesgo encontrado al interior del ICBF.

- Se documentaron las políticas de seguridad que se deben aplicar para la protección debida de los activos.

- Se realizaron los procedimientos de Backup, procedimientos de copia de seguridad, procedimiento de soporte técnico.

- Con el desarrollo de este proyecto se espera que la empresa implemente los controles y medidas que permitan lograr un nivel aceptable de seguridad.

BIBLIOGRAFIA

RAMIREZ VILLEGAS, G. M., & CONSTAIN MORENO, G. E. (2012). Modelos y Estandares de Seguridad Informatica. Palmira.

ROZO, E. A. (Enero de 2013). PROYECTO DE SEGURIDAD INFORMÁTICA I. La Plata, Huila, Colombia.

PORTAL DE ISO 27001 EN ESPAÑOL, 28 de Agosto del 2015, [En línea] http://www.iso27000.es/download/doc_sgsi_all.pdf.

ACADEMY, QUE ES LA ISO 27001. Tomado el día 29 de Agosto. [En línea] http://advisera.com/27001academy/es/que-es-iso-27001/.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, Tomado el día 29 de Agosto del 2015, [En línea]. http://www.iso27000.es/download/doc_sgsi_all.pdf.

QUINTERO JOSE LUIS ANALISIS Y GESTIÓN DEL RIESGO. Tomado el día 30 de Agosto del 2015, [En línea] http://www.aec.es/c/document_library/get_file?uuid=b3945e58-17f2-4dc0-88ac-863ae9f998cb&groupId=10128.

ISO 27001, ORIGEN E HISTORIA. Tomado el día 31 de Agosto del 2015. [En línea] http://www.pmg-ssi.com/2013/12/iso27001-origen/

HALABY WILLIAM, CAMBIOS RESPECTO A ISO 27001:2013, CHARTER COLOMBIA. Tomado el día 31 de Agosto del 2015. [En línea]. http://isc2capitulocolombia.org/portal/images/documents/ISO_27001-2013_ISC2_Colombia_Chapter.pdf

CORPORACION COLOMBIA DIGITAL, LEY DE PROTECCION DE DATOS PERSONALES: Una Realidad en Colombia. Tomado el día 1 de Setiembre del

2013. [En línea] http://colombiadigital.net/actualidad/noticias/item/4778-ley-de-proteccion-de-datos-personales-una-realidad-en-colombia.html.

LEYES INFORMATICAS EN COLOMBIA, UNAD. Tomado el día 14 de Abril del 2015, [En línea] http://gidt.unad.edu.co/leyesinformaticas

POVEDA JOSE MANUEL, Activos de Seguridad de la Información, Modulo 7, ISO 27001. Tomado el día 24 de Julio del 2015. [En línea]. http://www.worldvisioncapacitacion.cl/wp-content/uploads/cursos_adjuntos/f52e0bd4c6c2c203413952826f916237.pdf

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS, Oficina Asesora de Sistemas, Gestión del Riesgo, Capitulo 8, 10 de Agosto del 2015. [En línea] http://www.udistrital.edu.co:8080/documents/276352/356568/Cap5GESTIÓN Riesgo.pdf

UNAD, RIESGOS Y CONTROL INFORMATICO, Lección 1, Conceptos de Vulnerabilidad, Riesgos y Amenazas. Tomado el día 16 de Julio del 2015. [En línea]http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

BOLAÑOS, MARÍA C y ROCHA G. MONICA. 15 de Julio del 2015. MAGERIT V 3.0, (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). [En línea] http://es.slideshare.net/kinny32/magerit-v3-libro1metodo.

POVEDA JOSE MANUEL, Análisis y Valoración de los Riesgos, Modulo 8, ISO 27001. 30 de Julio del 2015. [En línea]. https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

BERNAL JIMENO JORGE, 20 de Agosto del 2015, CICLO PHCA (Planificar, Hacer, Verificar, Actuar): el circulo Deming de mejora continua (En línea) http://www.pdcahome.com/5202/ciclo-pdca.

MARCO LEGAL DE LA SEGURIDAD INFORMATICA EN COLOMBIA (línea) Disponible en: http://seguridadinformacióncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html

PORTAL WEB INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR, 20 de septiembre del 2014. (En línea), Disponible en: http:// www.icbf.gov.co.

TRIAS ZABALA SILVIA, Guía a la redacción en el estilo APA, 10 de Julio del 2015, [En línea], http://www.suagm.edu/umet/biblioteca/pdf/GuiaRevMarzo2012APA6taEd.pdf

FERRER RODRIGO, Sistema de Gestión de Seguridad de la Información. (En linea). Sisteseg.com: http://www.sisteseg.com/files/Microsoft_PowerPoint_-_Estrategias_de_seguridad_v52.pdf

MISFUD ELVIRA, Introducción a la Seguridad Informática, 12 de Agosto del 2015, [En línea], http://recursostic.educacion.es/observatorio/web/en/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1

UNIVERSIDAD NACIONAL DE LUJAN, Departamento de seguridad informática, 21 de Agosto del 2015, [En línea]. http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_GESTIÓN _de_riesgo.pdf

ICBF, PROCEDIMIENTO DE GESTIÓN DE SOLICITUDES TECNOLOGICAS, [en línea]. http://www.icbf.gov.co/portal/page/portal/IntranetICBF/macro_procesos/MP_apoyo/GESTIÓN _tecnologica/PR6.MPA6%20Gesti%C3%B3n%20de%20Solicitudes%20de%20Tecnologias%20de%20la%20Informaci%C3%B3n%20v3.pdf
`

ICBF, PROCEDIMIENTO DE GESTIÓN DE INCIENTES DE TECNOLOGIA DE LA INFORMACIÓN, tomado el día 27 de septiembre del 2015, [en línea]. http://www.icbf.gov.co/portal/page/portal/IntranetICBF/macro_procesos/MP_apoyo/GESTIÓN _tecnologica/PR9.MPA6%20Gesti%C3%B3n%20de%20Incidentes%20de%20Tecnolog%C3%ADas%20de%20la%20Inforamci%C3%B3n%20v1.pdf

ICBF, PROCEDIMIENTO DE GESTIÓN DE BACKUP, [en línea]. http://www.icbf.gov.co/portal/page/portal/IntranetICBF/macro_procesos/MP_apoyo/GESTIÓN _tecnologica/PR11-MPA6-GESTIÓN -Copias-de-Seguridad-v2_1.pdf

ICBF, PROCEDIMIENTO DE INCIDENTE MASIVO, tomado el día 25 de septiembre del 2015. [En línea]. http://www.icbf.gov.co/portal/page/portal/IntranetICBF/AplicacionesDIT/DIT%20-%20Base%20de%20Conocimiento/Base%20de%20conocimiento/Procedimiento%20Incidentes%20Masivos.pdf

ICBF, GUIA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO, tomado el día 2 de septiembre del 2015, [línea]. http://www.icbf.gov.co/portal/page/portal/IntranetICBF/macro_procesos/MP_apoyo/GESTIÓN _tecnologica/G6%20MPA6%20Gesti%C3%B3n%20Continuidad%20del%20Negocio%20v1.pdf

ANEXOS

ANEXO A: MANUAL DE POLITICAS DE SEGURIDAD

MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR, CENTRO ZONAL LA VIRGEN, REGIONAL BOLIVAR.

TABLA DE CONTENIDO

Pág.

1. INTRODUCCIÓN

Este documento describe las políticas y normas de seguridad de la información definidas por el ICBF, Centro Zonal Virgen y Turístico, Regional Bolívar. Para la elaboración del mismo, se toman como referencia la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.

Las políticas de seguridad presentes en este manual, son de gran importancia para el sistema de gestión de seguridad de la información, ya que son detallados los objetivos de control y controles a implementar permitiendo minimizar los riesgos encontrados en la empresa.

2. OBJETIVOS

Definir y explicar las políticas de seguridad de la información, permitiendo la protección de los activos de la empresa.

3. ALCANCE

Las políticas de seguridad cubre toda el área de la edificación del centro zonal, las áreas de trabajo de cada oficina, procedimientos de control que deben ser cumplidos por los directivos, usuarios internos y terceros que laboren en el ICBF.

4. DEFINICIONES

SEGURIDAD DE LA INFORMACIÓN: Es protección de la información contra las amenazas que tiene una empresa garantizando la continuidad del negocio y minimizando los riesgos a los que están expuesto los activos.[13]

LOS ACTIVOS: Son todos los elementos que contiene una empresa tales son: Los datos o información, servicios, aplicaciones (software), equipos (hardware), recursos físicos y recursos humanos.

AMENAZAS: Es cualquier situación que se puede presentar en la empresa dañando un activo mediante la presencia de una vulnerabilidad.[13]

VULNERABILIDAD: Debilidad de un activo que puede ser aprovechada por una amenaza.[13]

CONTROLES DE SEGURIDAD: Procedimiento de seguridad encargado de minimizar el riesgo.

CONFIDENCIALIDAD: Capacidad de no divulgar la información a personas no autorizadas.

RIESGOS: Es el daño que se le puede presentar a un activo cuando se encuentra desprotegido.

SGSI: Sistema de Gestión de Seguridad de la Información.

[13] SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, Tomado el día 29 de Agosto del 2015, [En línea]. http://www.iso27000.es/download/doc_sgsi_all.pdf.

RECURSOS TECNOLÓGICOS: Son las herramientas o medios informáticos el cual cumplen una función específica, pueden ser tangibles como un computador o intangible como una aplicación web.

CÓDIGO MALICIOSO: Son programas que afectan que vulneran la información de los sistemas informáticos, tales como virus, robo de información, espiar tus actividades en el PC entre otras.

SEGURIDAD FÍSICA: Es la seguridad aplicada a la infraestructura de una edificación y en las áreas internas tales como oficinas, almacén, bodegas entre otras.

SEGURIDAD DE LAS REDES: Es la seguridad aplicada a los recursos de comunicaciones de la red, desde configuraciones internas hasta perímetro físico de ubicación de los dispositivos de red.

COPIAS DE SEGURIDAD: Procedimiento para respaldar la información contra amenazas externas e internas.

CIFRADO DE INFORMACIÓN: Es encapsular la información mediante programas especiales para proteger su integridad.

DISPONIBILIDAD: Es la capacidad de mantener el activo de información disponible en el momento en que se requiera.

INTEGRIDAD: Mantener la información de manera intacta sin sufrir modificaciones.

5. POLITICA GLOBAL DE SEGURIDAD DE INFORMACIÓN.

En el ICBF, Centro zonal la Virgen, Regional Bolívar, protege, y preserva la integridad, confiabilidad y disponibilidad de la información física y digital, a través de la implementación de controles de seguridad, con el objetivo de garantizar el aseguramiento de la información de los procesos misionales propios de la entidad para que sea consultada, modificada únicamente por personas autorizadas de la empresa.[14]

6. POLITICAS DE ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO: Definir la seguridad de la información dentro de la organización.

6.1 NORMAS QUE RIGEN PARA LA ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN.

Normas Dirigidas a: FUNCIONARIOS Y DIRECTIVOS.

- Se debe promover el conocimiento de las políticas de Seguridad de la Información a todos los funcionarios de la empresa.
- Se debe establecer las responsabilidad de cada funcionario respecto a la actividades que cada quien maneja preservando la confidencialidad de la información.
- Los funcionarios deben aprender a clasificar la información de acuerdo al uso.

[14] ICBF, SISTEMA INTEGRADO DE GESTIÓN , 20 de septiembre del 2015, en línea. http://www.icbf.gov.co/portal/page/portal/IntranetICBF/contenido_misional/EPICO/sistema_integrado_de_GESTIÓN

Normas dirigidas a: OFICINA DE SISTEMAS Y TECNOLOGIA.

- Se debe analizar los incidentes de seguridad que se presenten para que sean Gestionados.
- La oficina de sistemas debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.
- La oficina de sistemas debe asignar las responsabilidades a sus funcionarios para la utilización de los recursos informáticos.

7. POLITICA DE RESPONSABILIDAD SOBRE LOS ACTIVOS.

OBJETIVO: Asegurar que se aplica un nivel alto de protección a los activos de la empresa.

Normas dirigidas a: OFICINA DE SISTEMAS Y TECNOLOGIA.

- Realizar y mantener configuración a los recursos informáticos de la empresa, para así hacer uso adecuado de ellos.
- Mantener un sistema de cifrado de información en medio magnético, protegiendo la información contra divulgación y modificaciones no autorizadas.
- Realizar inventario de equipos y aplicaciones.
- Realizar Backup de la información que manejan un usuario cuando es retirado del empleo.
- Se debe indicar a los funcionarios las condiciones de uso de los recursos informáticos manteniendo su disponibilidad e integridad.

Normas dirigidas a: EMPLEADOS Y DIRECTIVOS.

- Deben generar y mantener un inventario de los activos que están bajo su responsabilidad, lo cual debe cuidarlos.
- Establecer acuerdos de confidencialidad en los contratos, para prevenir que la información sea divulgada a terceras personas no autorizadas.
- Etiquetar la información de acuerdo a su clasificación.

8. POLITICA DE SEGURIDAD DIRIGIDA AL RECURSO HUMANO.

OBJETIVO: Asegurar que los funcionarios cumplan sus responsabilidades y obligaciones respecto a la política de seguridad, para reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

Normas dirigidas a: FUNCIONARIOS Y DIRECTIVOS.

- Deben colocar sanciones para aquellos funcionarios que no apliquen las políticas de seguridad.
- Informar al área de sistemas cuando un funcionario ha sido retirado del empleo.
- Cumplir con la aplicación de las políticas de seguridad establecidas en la empresa.

Normas dirigidas a: OFICINA DE SISTEMAS Y TECNOLOGIA.

- Debe programar de manera permanente campañas, capacitaciones que sensibilicen a los funcionarios sobre la importancia de la seguridad de la información.
- Debe contar con mecanismos que permita el traslado, reutilización o eliminación de los equipos.
- Debe cancelar las cuentas de acceso a los sistemas, cuando un funcionario ha sido retirado del empleo.

9. POLITICAS DE SEGURIDAD FISICA Y DEL ENTORNO.

9.1 AREAS SEGURAS.

OBJETIVO: Proteger los activos de la empresa contra amenazas físicas, humanas y del medioambiente, evitando la interrupción de las actividades misionales.

Normas dirigidas a: FUNCIONARIOS Y DIRECTIVOS.

- Mantener las puertas de las oficinas cerradas, para evitar el ingreso de personas no autorizadas.
- Se debe gestionar la adquisición de protección física contra incendios u otra clase de amenaza.

- Se debe informar a la oficina de sistemas cuando se requiera realizar traslado de equipos para otras oficinas, garantizando la protección del equipo

Normas dirigidas a: OFICINA DE SISTEMAS.

- Realizar vigilancia permanente a las personas que ingresen cuarto técnico de comunicaciones.
- Verificar que las políticas de seguridad física se estén cumpliendo.
- Supervisar que los equipos de comunicación estén en un cuarto libre de líquidos inflamables que no corran riesgo de inundaciones e incendios.
- Se debe implementar mecanismos de seguridad a la hora de hacer un traslado de equipo cuando un funcionario es ubicado en otra dependencia o área.

Normas dirigidas a: PERSONAL DE VIGILANCIA.

- Controlar el ingreso únicamente al personal autorizado.
- Deben registrar el acceso físico de visitantes que ingresen a la empresa.
- Mantener el registro diario del ingreso de portátiles o equipos tecnológicos ajenos al instituto.

9.2 SEGURIDAD EN LOS EQUIPOS.

OBJETIVO: Mantener la protección adecuada de los equipos para mantenerlos siempre disponibles en las actividades de la empresa.

Normas dirigidas a: OFICINA DE SISTEMAS.

- El equipo debe situarse en lugares fuera de amenazas externas.
- Mantener los equipos protegidos contra fallos en el suministro de energía, utilizando sistema de alimentación ininterrumpida (UPS).
- Se debe proteger el cableado para evitar roturas o daños en el servicio.
- Programar mantenimientos preventivos a los equipos de cómputos.

Normas dirigidas a: FUNCIONARIOS Y DIRECTIVOS.

- La dirección debe gestionar en adquirir equipos de plantas eléctricas para garantizar la continuidad del suministro eléctrico.
- No se debe sacar los equipos de cómputos fuera de las instalaciones de la empresa sin autorización de la oficina de sistemas.
- Dar buen uso a los equipos para que siempre disponibles.

10. POLITICA PARA LA GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES.

10.1 RESPONSABILIDAD Y PROCEDIMIENTOS DE OPERACIÓN.

OBJETIVO: Establecer y mantener los procedimientos de la operación de los procesos de la empresa.

Normas dirigidas a: OFICINA DE SISTEMAS.

- Debe mantener la documentación de los procedimientos de operación de la empresa y darlos a conocer a todos los funcionarios.

- Se deben dividir las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización.

10.2 SUPERVISION DE LOS SERVICIOS CONTRATADOS A TERCEROS.

OBJETIVO: Supervisión de la provisión de los servicios contratados o realizados a terceros para mantener la seguridad de la información.

Normas dirigidas a: FUNCIONARIOS Y DIRECTIVOS.

- Los contratos, acuerdos y convenios deben contar con las cláusulas de confidencialidad de la información para evitar que sea conocida a personas ajenas de la institución.
- Los jefes del área de deben monitorear y revisar los informes y registros suministrados por terceros.

10.3 PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA.

OBJETIVO: Supervisar los sistemas y recursos tecnológicos para minimizar el riesgo contra fallos.

Normas dirigidas a: OFICINA DE SISTEMAS.

- Debe Monitorizar y supervisar el uso de recursos tecnológicos, con el objeto de asegurar su funcionamiento.
- Adquirir e implementar mecanismos de información, actualización y desarrollar pruebas de sistemas nuevos durante el desarrollo y antes de su aceptación.

10.4 PROTECCIÓN CONTRA CÓDIGO MALICIOSO.

OBJETIVO: Aplicar controles adecuados para proteger la información de la empresa de software malicioso.

Normas dirigidas a: OFICINA DE SISTEMAS.

- Se debe implementar mecanismos de protección contra software malicioso.
- Instalar programa que bloqueo de código móvil en cada estación de trabajo para evitar la propagación de virus.
- Se debe mantener las últimas actualizaciones de los programas de protección contra software malicioso.

Normas dirigidas a: FUNCIONARIOS Y DIRECTIVOS.

- Se debe revisar las memorias USB con el antivirus al momento de ingresarla en el PC.
- Reportar alguna infección de software malicioso que detecten en sus computadores.

10.5 POLÍTICAS DE RESPALDO DE INFORMACIÓN.

OBJETIVO: Mantener la integridad y la disponibilidad de toda la información misional que se maneja en las actividades de la empresa.

Normas dirigidas a: OFICINA DE SISTEMAS

- Vigilar que se cumplan los procedimientos de copias de seguridad de toda la información esencial de la empresa.

- Se debe realizar de manera constante las copias de seguridad de la información que represente los procesos de gran importancia de la empresa.
- Mantener las copias de seguridad en un lugar seguro contra incendios, inundaciones u otra amenaza para garantizar la disponibilidad del uso de ellas.

Normas dirigidas a: FUNCIONARIOS Y DIRECTIVOS.

- El funcionario debe solicitar a la oficina de sistemas ayuda para el procedimiento de copias de seguridad e indicar cual información se debe respaldar.

10.6 POLITICA DE SEGURIDAD DE LAS REDES.

OBJETIVO: Proteger las redes contra las amenazas en los sistemas.

Normas dirigidas a: OFICINA DE SISTEMAS.

- Se debe implementar políticas de seguridad para proteger las redes y minimizar los riesgos frente a las amenazas existentes.
- Establecer normas de acceso a la red por parte de terceros.
- Velar por la confidencialidad de la información que se trasmite en el enrutamiento de las redes.

10.7 POLITICA DE MANIPULACIÓN DE LOS SOPORTES.

OBJETIVO: Establecer procedimientos para el manejo de los medios removibles y controlar el uso de ellos.

Normas dirigidas a: OFICINA DE SISTEMAS.

- Implementar mecanismos para proteger la manipulación de almacenamiento de la información, garantizando la confidencialidad, integridad y disponibilidad.
- Se debe establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados
- Se debe implementar sistemas de bloqueo de los puertos USB, para evitar la fuga de información esencial de la empresa.
- Proteger la documentación de los sistemas contra accesos no autorizados.

10.8 INTERCAMBIO DE INFORMACIÓN Y SOFTWARE

OBJETIVO: Establecer los procedimientos de intercambio de información de la empresa.

Normas dirigidas a: OFICINA DE SISTEMAS Y TECNOLOGIA.

- Adoptar herramientas para el cifrado de datos, evitando que sufran modificaciones.
- Establecer mecanismos de protección para la información contenida en los correos electrónicos.

- Aplicar `políticas o controles para proteger los sistemas de información de la empresa, evitar que sean manipulados.

  Normas dirigidas a: FUNCIONARIOS Y DIRECTIVOS.

- No está permitido comunicar información sensible de la empresa por vía telefónica.
- Se debe clasificar el uso de la información ya sea pública, uso interno o confidencial.
- Se debe adoptar controles al momento de realizar préstamos de documentación física a fin de proteger la información sensible contra modificaciones y pérdida.
- Se debe proteger los medios que contienen información contra acceso no autorizado o mal uso durante el trasporte fuera de las instalaciones de la empresa.

11. POLITICAS DE CONTROL DE ACCESO.

11.1 REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO.

OBJETIVO: Definir controles para el acceso a la información.

Normas dirigidas a: OFICINA DE SISTEMAS.

- Debe existir un procedimiento para cancelar el acceso a los sistemas de información, cuando se les informe que un usuario ha sido retirado del empleo.

Normas dirigidas a: FUNCIONARIOS Y DIRECTIVOS.

- Los Directivos deben informar a la oficina de sistemas el nivel de ingreso de cada funcionario a los sistemas de información de acuerdo al perfil establecido en el contrato.
- Desconectar las sesiones tras periodo de inactividad en los sistemas de información.

11.2 GESTIÓN DE ACCESO DE USUARIOS.

OBJETIVO: Establecer controles para el acceso de los usuarios a los sistemas de información.

- Mantener inventariado las cuentas de los usuarios tanto de los activos como de los que han sido retirado del empleo.
- Controlar la creación y uso de las cuentas de usuarios.
- Controlar la asignación y el nivel de privilegios de los usuarios a los sistemas de información.
- Establecer la asignación de contraseñas robustas a los usuarios y control del uso de ellas.

11.3 POLÍTICAS DE RESPONSABILIDAD DE LOS USUARIOS.

OBJETIVO: Definir los controles que son de responsabilidad de los funcionarios.

Normas dirigidas a: FUNCIONARIOS Y DIRECTIVOS.

- Aplicar las buenas prácticas de seguridad en el uso de las contraseñas.

- Bloquear el computador en el momento de quedar desatendidos.
- Mantener el escritorio libre de documentos físicos y las pantallas del PC limpias.
- Usar constantemente el carnet Institucional.
- Abstenerse de visitar páginas prohibidas ni tampoco almacenar información personal en los equipos de la empresa.
- Velar por el cuidado y buen uso de los recursos informáticos asignados.
- Todo el personal debe devolver los activos pertenecientes a la empresa en el momento de la cancelación del contrato laboral.
- Informar a la oficina de sistemas en el momento de presentar fallas en el software o hardware en los recursos informáticos.

11.4 CONTROL DE ACCESO EN RED.

OBJETIVO: Proteger la red contra accesos de personas no autorizadas que no pertenecen a la empresa.

Normas dirigidas a: FUNCIONARIOS Y DIRECTIVOS.

- Debe ingresar a la red solamente el personal que está autorizado para ingresar.

Normas dirigidas a: OFICINA DE SISTEMAS.

- Deben aplicar sistemas de autenticación para el control de acceso remoto.
- Se deben identificar cuáles son los equipos que pertenecen a la red y el lugar de ubicación de ellos.

- Se debe controlar la configuración y el acceso físico y lógico de los puertos.

11.5 CONTROL DE ACCESO AL SISTEMA OPERATIVO:

OBJETIVO: Controlar el acceso a los sistemas operativos mediante procedimientos de conexión.

- Todos los usuarios deben identificarse y autenticarse para el ingreso al sistema operativo, debe ser única y exclusiva de cada usuario.
- Se debe garantizar el uso de las contraseñas robustas para evitar el fraude en los sistemas.
- Se debe contar con software de gestión de seguridad que bloquee el acceso a programas utilitarios a usuarios no autorizados.
- Las secesiones se deben desconectar automáticamente tras un periodo de inactividad.

11.6 CONTROL ACCESO A LAS APLICACIONES.

OBJETIVO: Aplicar controles de protección para las aplicaciones de misión crítica de la empresa.

- Se debe restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones.

- Los sistemas de información sensible tales como el de financiera o liquidación debería de disponerse en un entorno información propia para mantener siempre la disponibilidad e integridad de la información.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

12.1 REQUISITO DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.

OBJETIVO: Aplicar controles de seguridad para los sistemas de información nuevos y ya existentes en la empresa.

- Se debe contar con procedimientos para la identificación de incidentes en los sistemas de información.

12.2 TRATAMIENTO CORRECTO DE LAS APLICACIONES.

OBJETIVO: Proteger contra el mal uso de la información que contiene los sistemas de información.

- Se deben validar los datos de entrada evitando el ingreso de datos incorrectos.

- Se debe asegurar la autenticación y protección de la integridad de los mensajes en las aplicaciones, implementando controles apropiados.

- Se debe validar los datos de salida de las aplicaciones para garantizar que el procesamiento de información almacenada sea correcta.

12.3 CONTROLES CRIPTOGRAFICOS.

OBJETIVO. Aplicar controles criptográficos para mantener la información disponible e integra.

- Se debe implementar una política para aplicar controles criptográficos a la información.

- Aplicar sistemas de claves para respaldar el uso de las técnicas criptográficas.

12.4 SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA.

OBJETIVO: Controlar la instalación de software en los computadores de la empresa.

- Se debe establecer procedimientos para controlar la instalación de software en los equipos de la empresa.

- Se debe restringir el acceso del código fuente de los programas.

12.5 MONITORIZACION EN LOS PROCESOS DE DESARROLLO Y SOPORTE.

OBJETIVO: Supervisar y monitorizar la información de las aplicaciones.

- Existir herramientas para prevenir la fuga de información.

- Deben existir procedimientos para la monitorización del software subcontratado en la empresa.

13. GESTIÓN DE INCIDENTES DE SEGURIDAD.

13.1 NOTIFICACION DE LOS EVENTOS DE SEGURIDAD.

OBJETIVO: Comunicar los eventos de seguridad que se presenten en la empresa.

- Se deben comunicar los incidentes de seguridad de información lo más posible mediante los procedimientos establecidos.

13.2 GESTIÓN DE INCIDENTES Y MEJORA EN LA SEGURIDAD DE LA INFORMACIÓN.

- Implementar mecanismos que permitan monitorear los tipos y costes de los incidentes en la seguridad de la información.

- Mantener las evidencias de los incidentes en dado caso si se requiera una investigación de lo ocurrido.

ANEXO B: PROCEDIMIENTOS DOCUMENTADOS.

INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR CENTRO ZONAL VIRGEN Y TURISTICO DE LA REGIONAL BOLIVAR

TABLA DE CONTENIDO

Pag.

1. PROCEDIMIENTOS DOCUMENTADOS

1.1 PROCEDIMIENTOS DE BACKUP.

Este procedimiento indica los pasos para solicitar el servicio de Backup en la empresa ICBF, Centro Zonal Virgen y Turístico.

1.1.1 OBJETIVO:

Establecer en la empresa la realización del Backup como medida de respaldo para garantizar la disponibilidad, integridad y confiabilidad de la información que se maneja.

1.1.2 ALCANCE:

Se inicia con la solicitud de copia de seguridad a la Mesa de Servicios, mediante el correo y finaliza con el envío de los medios magnéticos a custodia y cierre del requerimiento en la herramienta de Gestión de Servicios que utiliza la empresa para las solicitudes informáticas.[15]

1.1.3 DEFINICIONES:

BACKUP: Es una copia que se realiza a la información de la empresa como medida de respaldo en el momento que suceda un evento de seguridad.

MEDIO MAGNÉTICO: Es el recurso físico en el que se almacena la información generada por las copias de seguridad.

MEDIO EXTRAÍBLE: Dispositivo externo de almacenamiento que permite guardar la información contenida en un computador.

INGENIERO DE SISTEMAS REGIONAL: Persona encargada de atender, GESTIÓN ar y administrar los requerimientos de los sistema informáticos de la empresa.

MESA DE SERVICIO: Grupo de ingenieros que se encargan de registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información.[15]

LÍDER DE BACKUP: Es la persona encargada de velar porque la administración de los respaldos se realice de manera correcta según las políticas establecidas por el ICBF.[15]

FORMATO DE SOLICITUD DE BACKUP**:** Permite que los usuarios especifiquen los parámetros requeridos para la implementación correcta de un Backup programado.[15]

HERRAMIENTA DE GESTIÓN DE SERVICIO: Son todos los sistemas, aplicaciones, controles, soluciones de cálculo, metodología, etc., que ayudan a la gestión de una empresa; para el caso de TI para el manejo y control de servicios es el software en donde se documentan los servicios de gestión tecnológica.[15]

INGENIERO DE SOPORTE EN SITIO: Persona encargada de brindar soporte en las diferentes sedes del ICBF.[15]

INGENIERO REGIONAL: Persona encargada de dar soporte tanto técnico como profesional a los usuarios sobre el uso de las herramientas tecnológicas y los sistemas de información del ICBF.[15]

1.1.4 CONDICIONES GENERALES.

El Líder de Backup debe definir y dar cumplimiento a la política de Backup de la entidad, una vez el funcionario solicite el servicio, el ingeniero de sistemas debe dejar registro del Backup realizado mediante el formato establecido.[15]

1.1.5 DESCRIPCION DEL PROCEDIMIENTO.

El procedimiento que se describe a continuación es de uso exclusivo del ICBF, el cual reposa en la intranet de la empresa y en la página web, indicada en la referencia.

Tabla 24: Procedimiento de Gestión de copias de seguridad.[15]

N	ACTIVIDAD	RESPONSABLE	REGISTRO
1	Funcionario solicita el Backup a la mesa de servicio, mediante el correo.	Ingeniero de sistemas, Coordinador del centro zonal.	Formato de solicitud de Backup.
2	¿El formato de solicitud se encuentra correctamente diligenciado y solicitado por una persona autorizada? **Sí:** Continuar al paso 3 **No:** Regresar el formato al solicitante y recibirlo solo hasta que cuente con las condiciones mínimas requeridas, volver paso 1	Mesa de servicio,	Herramienta de gestión de servicio.
3	Remitir el caso al Líder de Backup.	Mesa de servicio.	Herramienta de gestión de servicio.
4	Validar con el Líder de Backup del ICBF, el cual aprueba la realización del respaldo.	Mesa de servicios	Correo Electrónico
5	Remitir el requerimiento al Ingeniero de		

[15] ICBF, PROCEDIMIENTO DE GESTIÓN DE COPIAS DE SEGURIDAD, tomado el día 28 de septiembre del 2015. [en línea]. http://www.icbf.gov.co/portal/page/portal/IntranetICBF/macro_procesos/MP_apoyo/GESTIÓN_tecnologica/PR11-MPA6-GESTIÓN -Copias-de-Seguridad-v2_1.pdf

	sistemas de la regional de acuerdo a la ubicación o las condiciones en las que se solicita el servicio.	Líder de Backup	Herramienta de Gestión de Servicios
6	El ingeniero recibe la solicitud y realiza el respaldo de la información de acuerdo al formato enviado por el solicitante del respaldo, verificando su integridad.	Ingeniero de sistemas Regional, ingeniero de soporte.	Medio extraíble.
7	Enviar los medios magnéticos a custodia de la oficina de sistemas de la regional cada vez que se requiera e informar al Líder de Backup.	Ingeniero de sistemas Regional, Ingeniero de soporte.	Oficinas de sistemas.
8	Cierre del requerimiento	Ingeniero de sistemas Regional.	Herramienta de gestión de servicios.

Fuente: El autor.

1.1.6 RESPONSABILIDADES

- Los funcionarios del ICBF, realizan las solicitudes de Backup mediante el formato indicado.
- El ingeniero Regional e Ingeniero de soporte en sitio son los encargados de atender el servicio y documentarlo en la herramienta de gestión de servicio de acuerdo a la solicitud recibida de parte del funcionario.[15]
- El Líder de Backup se encargará de validar y configurar las solicitudes de acuerdo a los formatos recibidos a través de la mesa de servicio.[15]
- Mesa de servicios: Atender el requerimiento de la solicitud del servicio en la herramienta de gestión de servicios.[15]

1.1.7 DURACION DEL PROCEDIMIENTO:

Para el caso de respaldo a información contenida en los computadores de los funcionarios, la atención del servicio de este requerimiento con la mesa de servicios y los ingenieros regionales generalmente dura 1 día. [15]

1.2 PROCEDIMIENTO DE SOLICITUD DE CORREO INSTITUCIONAL.

Este procedimiento indica como el funcionario debe solicitar el servicio de creación de cuenta de correo.

1.2.1 OBJETIVO

Definir el procedimiento para la creación de cuenta de correo institucional.

1.2.2 ALCANCE

Inicia desde el ingreso de una solicitud a través de un medio de comunicación y termina con la entrega de la cuenta de correo al grupo solucionador del procedimiento correspondiente.[16]

1.2.3 DEFINICIONES DE TERMINOS

CUENTA DE USUARIO: Cuenta asignada al usuario para poder registrarse y realizar las actividades asignadas.

CORREO ELECTRONICO: Herramienta tecnológica de comunicación que permite envío y recepción de información mediante la red.

INGENIERO REGIONAL: Persona encargada de dar soporte tanto técnico como profesional a los usuarios sobre el uso de las herramientas tecnológicas y los sistemas de información del ICBF.[15]

MESA DE SERVICIO: Grupo de ingenieros que se encargan de registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados,

requerimientos de servicio y solicitudes de información.[15]

HERRAMIENTA DE GESTIÓN DE SERVICIO: Son todas las aplicaciones, controles, soluciones de cálculo, metodología, entre otras, que ayudan a la gestión de una empresa; para el caso de TI para el manejo y control de servicios, es el software en donde se documentan los servicios de gestión tecnológica.[15]

TICKET O NÚMERO DE SERVICIO: Número consecutivo suministrado por una Herramienta de Gestión durante el reporte de una Solicitud de Servicio, para facilitar a través del mismo el seguimiento y control.[15]

COORDINADOR DEL CENTRO ZONAL: Persona encargada de dirigir y administrar el centro zonal.

1.2.4 DESCRIPCION DEL PROCEDIMIENTO

El procedimiento que se describe a continuación es de uso exclusivo del ICBF y se encuentra definido en la intranet de la empresa y en la página web institucional especificada en la referencia.

Tabla 25: Procedimiento de solicitud de correo electrónico.[16]

N	ACTIVIDAD	RESPONSABLE	REGISTRO
1	Solicitan el servicio de creación de cuenta de correo.	Coordinadora del centro zonal.	Correo electrónico
2	2.1 Identificar una solicitud de servicio que requiera solución. 2.2 Enviar la solicitud a la Mesa de Servicio ya sea telefónicamente o por correo electrónico con el fin de obtener la solución del mismo.	Ingeniero de sistemas, Coordinador del Centro Zonal.	. Herramienta de Gestión de Servicios
3	3.1 Recibir la solicitud de servicio, registrarla en la Herramienta de Gestión y clasificarla según corresponda. 3.2 Categorizar y priorizar la solicitud de servicio con el fin de ser enviada al Procedimiento para la Gestión de Requerimientos de Tecnologías de la Información y finalizar.	Mesa de servicio e ingeniero regional.	Herramienta de gestión de servicio.
4	Validar la creación de la cuenta de correo, verificación de los datos con el usuario.	Ingeniero Regional.	Teléfono
5	Se procede a GESTIÓN ar la creación de la cuenta de correo.	Ingeniero Regional.	Correo electrónico.
6	Se envía la cuenta de correo creada al ingeniero de la sede o coordinadora de grupo.	Ingeniero regional.	Correo electrónico
7	Ingenieros recibe la cuenta de correo creada	Ingeniero Regional.	Documento digital.
8	Cierre del requerimiento	Ingeniero Regional.	Herramienta de Gestión de Servicio

Fuente: El autor.

[16] ICBF, PROCEDIMIENTO DE GESTIÓN DE SOLICITUDES TECNOLOGICAS, tomado el día 29 de septiembre del 2015, [en línea].
http://www.icbf.gov.co/portal/page/portal/IntranetICBF/macro_procesos/MP_apoyo/GESTIÓN_tecnologica/PR6.MPA6%20Gesti%C3%B3n%20de%20Solicitudes%20de%20Tecnologias%20de%20la%20Informaci%C3%B3n%20v3.pdf

1.2.5 DURACION DEL CICLO DE PROCEDIMIENTO

El tiempo total trascurrido para el proceso de creación de cuenta de correo son de 1 días.

1.2.6 RESPONSABILIDADES.

- Coordinador del centro zonal, quien solicita la creación de la cuenta de correo.
- Mesa de servicio, recibe la solicitud mediante la herramienta de gestión.
- Ingeniero Regional: Recibe requerimiento ya realizado por parte del líder de cuenta de correo.
- El ingeniero Regional e Ingeniero de soporte en sitio son los encargados de atender el servicio y documentarlo en la herramienta de gestión de servicio de acuerdo a la solicitud recibida de parte del funcionario.[15]

1.3 PROCEDIMIENTO DE SOLICITUDES TECNOLOGICAS.

Este procedimiento indica la manera de realizar una solicitud de soporte técnico a la oficina de sistemas del ICBF, Centro Zonal Virgen y Turístico.

1.3.1 OBJETIVO.

Atender y Gestionar las solicitudes de servicios tecnológicos mediante medios electrónicos asignadas al personal encargado.

1.3.2 ALCANCE

Inicia desde el ingreso de una solicitud a través de cualquier medio de comunicación (teléfono, correo, servicio web) y termina con la asignación según el tipo de solicitud al grupo solucionador del procedimiento correspondiente.[16]

1.3.3 DEFINICION DE TERMINOS:

INGENIERO REGIONAL: Persona encargada de atender, gestionar y administrar los requerimientos de los sistema informáticos de la empresa.[15]

GESTIÓN DE REQUERIMIENTOS DE TECNOLOGÍAS DE LA INFORMACIÓN: Procedimiento responsable del control del Ciclo de Vida de todos los cambios estándar.[16]

MESA DE SERVICIO: Grupo de ingenieros que se encargan de registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información.[15]

HERRAMIENTA DE GESTIÓN DE SERVICIO: Son todas las aplicaciones, controles, soluciones de cálculo, metodología, entre otras, que ayudan a la gestión de una empresa; para el caso de TI para el manejo y control de servicios, es el software en donde se documentan los servicios de gestión tecnológica.[15]

TICKET O NÚMERO DE SERVICIO: Número consecutivo suministrado por una Herramienta de Gestión durante el reporte de una Solicitud de Servicio, para facilitar a través del mismo el seguimiento y control.[15]

FORMATO DE SOLICITUD: Formato indicado de obtener información de la solicitud del usuario, especificando la solicitud requerida e incidente a reportar[16]

1.3.4 DESCRIPCION DEL PROCEDIMIENTO:

El procedimiento que se describe a continuación es de uso exclusivo del ICBF y se encuentra definido en la intranet de la empresa y en la página web institucional especificada en la referencia.

Tabla 26: Procedimiento de solicitudes tecnologicas.[16]

N	ACTIVIDAD	RESPONSABLE	REGISTRO
1	Funcionario envía la solicitud de soporte técnico, solicitando el servicio. Si la solicitud es por escrito, funcionario diligencia un formulario si no continua al paso 3.	Funcionarios de la empresa.	Correo electrónico, Teléfono o página web.
2	¿El formato de solicitud se encuentra correctamente diligenciado y solicitado por una persona autorizada? Si: continúa al paso 3. No: Volver a realizar solicitud.	Mesa de servicio,	Herramienta de gestión de servicio.
4	Recibir la solicitud de servicio, registrarla en la Herramienta de Gestión y clasificarla según corresponda.	Grupo ingenieros de la regional, Mesa de servicio,	Herramienta de gestión de servicio.
5	**¿La solicitud de servicio es un Incidente?** Si: Categorizar y priorizar la solicitud de servicio con el fin de ser enviada al Procedimiento para la Gestión de Incidentes de Tecnologías de la Información y finalizar. No: Verificar que otro tipo de solicitud está realizando el solicitante. 2.2 Verificar si la solicitud de servicio corresponde a un cambio pre-aprobado.	Mesa de servicios	Herramienta de gestión de servicio.
	¿La solicitud de servicio es un cambio pre-aprobado?		

6	Si: Categorizar y priorizar la solicitud de servicio con el fin de ser enviada al procedimiento para la Gestión de Requerimientos de tecnologías de la Información y finalizar. No: Categorizar y priorizar la solicitud de servicio con el fin de ser enviada al Procedimiento para la Gestión de Cambios de Tecnologías de la Información y Finalizar.	Mesa de servicios	Herramienta de gestión de servicio.
7	Se asigna la solicitud de pre-aprobado al grupo de ingenieros de la regional.	Mesa de servicios	Herramienta de gestión de servicios.
8	Proceden a atender la solicitud.	Ingenieros de la regional.	Centro Zonal.
9	Cierre del requerimiento	Ingeniero Regional.	Herramienta de Gestión de Servicio

Fuente. El autor.

1.3.5 DURACION DEL PROCEDIMIENTO:

La duración máxima del servicio debe durar como máximo 1 día.

1.3.6 RESPONSABILIDADES:

- Los funcionarios solicitan el servicio de soporte tecnológico mediante el correo.
- Mesa de servicio: Registra la solicitud de servicio mediante la herramienta gestión de servicios.
- El Ingeniero de sistemas Regional y el Soporte en sitio reciben la solicitud del servicio mediante la herramienta de gestión.

2. PLAN DE GESTIÓN DE INCIDENTES

Definir los pasos para la atención de incidentes presentados en la empresa, el cual se considera una labor de carácter prioritario debido al impacto que genera a los usuarios y a la restauración del servicio.

2.1 OBJETIVO

Recuperar el normal funcionamiento de los servicios informáticos en el menor tiempo posible, a través de diagnóstico, investigación y escalamiento de incidentes para mantener la calidad y la disponibilidad del servicio.[17]

2.2 ALCANCE

Inicia con el registro del incidente de seguridad en la herramienta de gestión de Servicios y termina con la verificación que el incidente este bajo control.[16]

2.3 DEFINICION DE TERMINOS:

INCIDENTE DE SEGURIDAD: Es un evento que se presenta en la empresa de manera inesperada causando daño a los activos de información afectando la disponibilidad, integridad y confiabilidad.

GRUPO DE ANALISTA DE INCIDENTES: Grupo de ingenieros encargados especialmente de atender las solicitudes de incidentes que se presenten.[17]

MESA DE SERVICIO: Grupo de ingenieros que se encargan de registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información.[15]

HERRAMIENTA DE GESTIÓN DE SERVICIO**:** Son todos los sistemas, aplicaciones, controles, soluciones de cálculo, metodología, etc., que ayudan a la gestión de una empresa; para el caso de TI para el manejo y control de servicios, es el software en donde se documentan los servicios de gestión tecnológica.[15]

BASE DE DATOS DE CONOCIMIENTO: Es un repositorio de información para consultar instructivos, manuales, artículos, soluciones a incidentes o problemas ya resueltos y otros temas acerca del servicio.[15]

REGISTRO DEL INCIDENTE: Es un conjunto de datos con todos los detalles de un Incidente que documenta la historia de los mismos desde su registro hasta su resolución.

INCIDENTE NORMAL: Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de la calidad de dicho servicio.[17]

INCIDENTE MAYOR**:** Falla en el servicio que causa alto impacto en la operación y que debe ser atendido con mayor grado de urgencia que un incidente normal.[17]

GESTIÓN DE SOLICITUDES DE TECNOLOGIA DE LA INFORMACIÓN**:** Procedimiento responsable de evaluar, analizar de forma rápida y eficiente la solicitud de servicio presentada por el solicitante, que requiera solución.[17]

PROBLEMA: Es la causa de uno o más incidentes. No es frecuente conocer su causa, por lo tanto es necesario realizar su investigación.[17]

PROPIETARIO DE INCIDENTE: Funcionario que recibe el incidente y hace un diagnóstico previo. Puede cumplir este rol la Mesa de Servicio o un nivel de escalamiento superior.[17]

TICKET O NÚMERO DE SERVICIO: Número consecutivo suministrado por una Herramienta de Gestión durante el reporte de una Solicitud de Servicio, para facilitar a través del mismo el seguimiento y control.[15]

ANALISIS DE CAUSA RAIZ: Es una actividad que identifica la raíz o causa de un incidente.[17]

2.4 PROCEDIMIENTO PARA LA ATENCION DE UN INCIDENTE.

El procedimiento que se describe a continuación es de uso exclusivo del ICBF y se encuentra definido en la intranet de la empresa y en la página web institucional especificada en la referencia.

Tabla 27: Procedimiento de atención a incidente.[17]

N	ACTIVIDAD	RESPONSABLE	REGISTRO
1	1.1 Registrar y categorizar el Incidente en la Herramienta de Gestión. 1.2 Verificar, si la solicitud no es un incidente pasar al Procedimiento Gestión de Solicitudes de Tecnologías de la Información y Finalizar. 1.3 Validar el tipo de Incidente: Incidente normal o incidente mayor. 1.3.1 Realizar las notificaciones correspondientes a los Grupos de Solución. 1.4 Validar si existe una solución temporal o definitiva disponible para ejecutar en el servicio. **¿Existe una solución?** Si: Pasar a 2.2 No: Re categorizar y priorizar el incidente con el fin de documentar el servicio y pasar al Analista.	Funcionarios de la empresa, ingeniero de sistemas de la regional.	Herramienta de gestión.
2	2.1 Analizar, diagnosticar e investigar el incidente que no tiene solución. 2.1.1 Crear o ejecutar una solución rápida y efectiva al mismo. 2.1.2 Verificar la información documentada con el fin de contactar al usuario en caso de requerir información adicional para la solución de incidente. 2.1.3 Validar si es necesario generar un análisis de causa raíz o crear una solución alternativa con el fin de dar solución al incidente. **¿Necesario un Análisis de Causa Raíz o Solución Alternativa?** Si: Realizar el Análisis de Causa Raíz o crear una solución alternativa dentro del Procedimiento de Gestión de Problemas de Tecnologías de la Información con el fin de implementarlo dentro de este procedimiento y pasar a 2.2.	Analista de incidente, Mesa de servicio, grupo de ingenieros de sistemas de la regional.	Herramienta de gestión de servicio

[17] ICBF, PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE TECNOLOGIA DE LA INFORMACIÓN, tomado el día 28 de septiembre del 2015. [en línea].
http://www.icbf.gov.co/portal/page/portal/IntranetICBF/macro_procesos/MP_apoyo/GESTIÓN_tecnologica/PR9.MPA6%20Gesti%C3%B3n%20de%20Incidentes%20de%20Tecnolog%C3%ADas%20de%20la%20Inforamci%C3%B3n%20v1.pdf

	No: Continuar. 2.1.5 Validar si para la implementación de la solución del incidente se hace necesario un cambio a nivel informático, en caso afirmativo generar la solicitud de cambio o la solicitud de desarrollo dentro del Procedimiento de Cambios de Tecnologías de la Información. 2.2 Resolver el incidente con el fin de dar disponibilidad al Usuario. 2.3 Obtener la aprobación del Usuario final para el cierre del registro del incidente. **¿Usuario Final autoriza el cierre del incidente?** Si: Actualizar el registro del incidente e ir a la actividad 2.4 No: Pasar a 2.1 2.4 Verificar si la solución del incidente fue temporal y si es necesario un Análisis de causa raíz con el fin de resolverlo de forma definitiva. **¿Requiere un Análisis de Causa Raíz?** Si: Realizar el Análisis de Causa Raíz dentro del Procedimiento de Gestión de Problemas de Tecnologías de la Información y Finalizar. No: Pasar a 2.5 2.5 Validar si la solución implementada debe ser ingresada dentro de la Base de Datos de Conocimientos y en caso afirmativo realizar la actualización de la base de datos de conocimientos dentro del Procedimiento de Gestión de Problemas de Tecnologías de la Información.		

Fuente. El autor.

2.5 CLASIFICACION DE INCIDENTES.

Cada funcionario, proveedor o tercero que esté en contacto con información del ICBF, Centro Zonal virgen y Turístico debe reportar toda clase de incidente o evento que pudiera causar pérdidas o daños en los sistemas informáticos y en la información que manejan.

Existen 2 clases de incidentes, los que se caracterizan por causar daños en los activos, que son los de mayor nivel y los de menor nivel que no afectan la continuidad del servicio de la empresa.

2.6 TRATAMIENTO DE INCIDENTES MENORES.

Los Incidentes Menores no interrumpen la calidad del servicio de la empresa sin causar daño alguno, se debe dar respuesta en máximo una hora al usuario.[17]

2.6.1 CICLO DE VIDA PARA TRATAR A UN INCIDENTE MENOR

- **Grupo de Soporte a Gestión de Incidentes:** Reciben los incidentes reportados, analizan, verifican y luego son remitido a la mesa de servicios.[17]

- **Registro y Categorización:** El grupo de soporte de gestión registra y clasifica el incidente sobre la herramienta de gestión y remite el incidente al ingeniero de sistemas de la regional, de esta manera facilita las soluciones eficientes e inmediatas.[18]

- **Análisis**: El ingeniero de sistemas de la regional, analizan la solución más conveniente y rápida.

- **Solución del incidente:** Atienden el incidente menor, se debe restablecer en el tiempo establecido.[17]

- **Cierre de incidente:** Se procede al cierre después de haber superado el incidente.[17]

- **Registro del incidente:** Se registra en la base de conocimiento como medida de solución rápida en caso que se vuelva a presentar nuevamente el evento.[18]

2.7 TRATAMIENTO DE INCIDENTES MAYORES.

Los Incidentes Mayores pueden afectar la integridad y disponibilidad de los activos de información de la empresa, por lo cual requiere de atención pronta ya que probablemente genera la suspensión de las actividades laborales.

2.7.1 CICLO DE VIDA PARA TRATAR A UN INCIDENTE MAYOR.

Los incidentes mayores son aquellos que afectan a más de 5 usuarios en la empresa. A continuación se describen los procedimientos de atención a incidente mayor en cual es exclusivo del ICBF.[18]

- **Detección o Identificación:** Al identificar un incidente mayor, se debe informar al gestor de incidentes para que éste realice la verificación, análisis de la prioridad del caso conforme a la matriz de prioridades para así realizar el tratamiento debido del caso.[18]

[18] ICBF, PROCEDIMIENTOS DE INCIDENTES MASIVOS, tomado el día 29 de septiembre del 2015, [en línea]. http://www.icbf.gov.co/portal/page/portal/IntranetICBF/AplicacionesDIT/DIT%20-%20Base%20de%20Conocimiento/Base%20de%20conocimiento/Procedimiento%20Incidentes%20Masivos.pdf

- **Grupo de Soporte a Gestión de Incidentes:** Reciben los incidentes reportados, analizan, verifican y luego son remitido a la mesa de servicios.[18]

- **Registro y Categorización:** El grupo de soporte de gestión registra y clasifica el incidente sobre la herramienta de gestión, realiza la documentación y categorización según el servicio que esté afectado.[18]

- **Categorización:** Las categorizaciones sobre la herramienta de Gestión se basan en el diagnóstico del agente que lo recibe y a la vez clasifica el incidente conforme al análisis de primer nivel. Este a su vez puede ser re categorizado por el usuario asignado para solucionar el incidente quien en un escalamiento de segundo nivel identifica plenamente la raíz de la Incidencia a un grupo solucionador del problema.[18]

- **Investigación y Diagnostico:** El grupo resolutor al recibir el Incidente Masivo entra a investigar y a diagnosticar la causa de la falla e inicia validando el estado del servicio que administra. Si la revisión de la afectación necesita la participación de varios grupos solucionadores estos son participes de las actividades a realizar para la restauración del servicio.[18]

- **Elevación de un incidente mayor a problema:** Cuando la incidencia no tiene una solución temporal se considera un incidente mayor, por lo cual se eleva el proceso desde la plantilla de incidencias al gestor de problemas vía correo electrónico se notifica incluyendo al grupo de interesados sobre la restauración del servicio.[18]

- **Cierre de incidentes mayor:** Se cierra con la recuperación de la operatividad del servicio afectado, mediante un informe generado por parte del grupo resolutor asignado quien determina su correcto funcionamiento.[18]

- **Registro del incidente:** se registra en la base de conocimiento como medida de solución rápida en caso que se vuelva a presentar nuevamente el evento.[18]

2.8 APRENDIZAJE A PARTIR DE LOS INCIDENTES.

Para el proceso de aprendizaje y mejorar los procesos en atención a próximos incidentes, el equipo de respuestas a incidentes debe mantener y crear una base de conocimiento de incidentes en la cual se consignen los reportes de incidentes y la solución dada a los mismos, que sirva en un futuro como primera alternativa de consulta en la resolución de incidentes informáticos con información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados, y experiencias con incidentes anteriores.

De esta manera con la base de conocimiento se implementan medidas preventivas para que no vuelva a ocurrir el incidente y también para educar a los funcionarios.

2.9 MEDIDAS DISCIPLINARIAS.

Cuando la oficina de sistemas identifique que un funcionario ha generado brechas de seguridad o ha participado en eventos para generar incidentes, se debe a incumplimiento de las políticas de seguridad establecidas en la empresa, de acuerdo a la situación presentada se emitirá un reporte a la oficina de control interno y al departamento de recursos tecnológicos, el cual tiene como consecuencia una sanción disciplinaria dependiendo de la naturaleza de gravedad del caso, podría atribuirse como violaciones graves, robo de información daño, divulgación de información reservada del instituto o se declare culpable de un delito en específico.

3. GESTIÓN DE CONTINUIDAD DEL NEGOCIO.

3.1 OBJETIVO.

Definir los pasos que se deben seguir para contrarrestar los eventos que afecten los requisitos de seguridad en los sistemas de información manteniendo la continuidad del negocio y asegurar la recuperación oportuna del funcionamiento de los recursos del l ICBF, Centro zonal Virgen y Turístico. [19]

3.2 ALCANCE.

Inicia con la identificación de los eventos que pueden ocasionar interrupciones de los procesos misionales, definir los planes de acción, los tiempos de recuperación y objetivos de recuperación, y la realización de las pruebas periódicas de estos planes definidos.[19]

3.3 DEFINICION DE CONCEPTOS.

INCIDENTE DE SEGURIDAD: Situación que podría causar la interrupción del negocio, pérdidas, emergencia o crisis, debido a la presencia de vulnerabilidades.

INTRUSIÓN DE SEGURIDAD: Violación de controles o normas de seguridad aplicadas en un área específica.

[19] ICBF, GUIA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO, tomado el día 2 de septiembre del 2015, [línea]. http://www.icbf.gov.co/portal/page/portal/IntranetICBF/macro_procesos/MP_apoyo/GESTIÓN _tecnologica/G6%20MPA6%20Gesti%C3%B3n%20Continuidad%20del%20Negocio%20v1.pdf

VIOLACIÓN DE SEGURIDAD: Interceptar, destruir, las barreras de seguridad para ingresar de manera agresiva a un sistema informático.

CERT: Centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.[20]

AMENAZA: Situación o evento natural que compromete a los activos de la empresa, afectando su disponibilidad.

CONTINUIDAD DEL NEGOCIO: Capacidad de responder a incidentes o amenazas, con el fin de continuar las operaciones de la empresa, logrando así el mínimo impacto a la operación del negocio.

PLAN DE CONTINUIDAD DEL NEGOCIO: Conjunto de procedimientos e información documentados que se desarrolla, compila y mantiene preparado para su utilización en caso de producirse un incidente, para permitir a la organización continuar desempeñando sus actividades críticas a un nivel aceptable predefinido.[19]

COMITÉ OPERATIVO DE EMERGENCIAS (COE): Grupo administrativo de las emergencias antes, durante y después de los eventos; responsable de organizar planear y poner en funcionamiento el plan de emergencias.[21]

[20] WIKIPEDIA, EQUIPO DE RESPUESTAS ANTE EMERGENCIA INFORMATICA, tomado el día 29 de septiembre del 2015, [en línea]
https://es.wikipedia.org/wiki/Equipo_de_Respuesta_ante_Emergencias_Inform%C3%A1ticas
[21] ICBF, REGIONAL BOLIVAR, PLAN DE PREPARACION Y RESPUESTA ANTE EMERGENCIA, tomado el día 29 de septiembre del 2015, en línea,
http://www.icbf.gov.co/portal/page/portal/IntranetICBF/macro_procesos/MP_apoyo/G_soporte/G_human

CONTINGENCIA: Evento que ocurre en la mayoría de los casos en forma repentina o inesperada.[21]

BRIGADA DE EMERGENCIAS: Grupo operativo con entrenamiento para atender emergencias incipientes.

ALERTA: Período anterior a la ocurrencia de un desastre, declarado con el fin de tomar precauciones específicas, debido a la probable y cercana ocurrencia un desastre.[21]

IMPACTO**:** Es el daño que se produce en un activo cuando sucede una amenaza.

RIESGO: Es el daño que se le puede presentar a un activo cuando se encuentra desprotegido.

3.4 CAUSAS DE INTERRUPCION.

Los planes de contingencia se definen de acuerdo con las causas de las posibles interrupciones y a partir de ellas se presentan las acciones a seguir.

---

a/PlanesModelos/PP124.MPA1.P1%20PLAN%20DE%20PREPARACI%C3%93N%20Y%20REGIONAL%20BOLIVAR.pdf

- Ausencia de Personal: Se presenta cuando el funcionario no puede asistir a sus tareas laborales propias de su cargo.

- No acceso al sitio normal de trabajo: Se presenta cuando el personal no puede acceder a su lugar de trabajo debido a algún evento como desastre natural, actividad terrorista, problemas de transporte, huelgas, entre otros.

- Fallas de los sistemas tecnológicos: Se refiere a los problemas tecnológicos en el hardware y/o software presentando fallas de funcionamiento.

- No contar con los Proveedores Externos: Se presenta cuando el proveedor falla antes sus responsabilidades ocasionando inconvenientes en la empresa.

- Corte o falta de fluido eléctrico: se presenta cuando hay ausencia de energía, de esta manera hay suspensión del trabajo laboral.

3.5 COMITE ENCARGADO DEL PROCESO.

El comité encargado de los procesos de atención al plan de Continuidad del negocio en caso de materializarse un evento, descritos a continuación es de uso exclusivo del ICBF y está conformado por los siguientes grupos. [19]

- Comité Directivo de Emergencia.
- Brigadistas.
- Equipo de soporte a usuario.
- Equipo de respuesta a incidentes.
- Equipo de recuperación de contingencias.

3.6 ROLES Y RESPONSABILIDADES

Las funciones de cada grupo descritas a continuación son de uso exclusivo del plan de preparación y respuestas ante emergencia del ICBF, Regional Bolívar, y se encuentra disponible en la referencia indicada.[21]

- **Comité Directivo de Emergencia:** Grupo de expertos en atención de emergencias, encargado de coordinar y tomar las decisiones necesarias antes, durante y después de la emergencia.

  Funciones:

- Asumir la dirección y control de la emergencia, en su respectivo puesto de comando.
- Determinar si la emergencia requiere evacuación total, parcial o no requiere evacuación de los colaboradores.
- Ordenar la activación de la alarma, en caso de una evacuación total.
- Hacer cumplir la operatividad del plan y promover su divulgación a los colaboradores.
- Asegurar que se mantengan los correctivos del plan de emergencias.
- Asegurar la actualización del documento del plan de emergencias.
- Establecer vínculos con los organismos de socorro de la en caso que sea necesario.

- **Brigadistas:** Es el grupo encargado de atender la evacuación del personal de la empresa en caso de una emergencia, estas funciones se encuentran disponibles en la referencia indicada.[21]

Funciones:

- El Brigadista debe conocer los riesgos generales y particulares que se presentan en los diferentes sitios y actividades que se desarrollan en el área en que labora y además debe conocer los riesgos a nivel general.
- Informará al Jefe sobre las posibles situaciones que constituyan riesgo y/o afecten los mecanismos de protección (extintores) y además verificará que se eliminen o solucionen adecuadamente.
- Conocer la existencia y uso correcto de los mecanismos de protección (alarmas, extintores), disponibles en el área en que labora y de toda la Regional Bolívar.
- Inspeccionar periódicamente las áreas
- Realizar Inventario e Inspección periódica de equipos contra incendio
- Asistir a capacitaciones que se programen
- Realizar prácticas para actualización
- Realizar entrenamiento físico

- **Equipo de soporte a usuario:** Grupo de ingenieros de sistema conformado por mesa de servicio, soporte técnico e ingenieros de sistemas de la regional, encargados de atender, gestionar y solucionar los requerimientos de TI, a continuación se presentan las funciones que son exclusivas del ICBF, se detallan en la siguiente referencia. [22]

Funciones o Responsabilidades:

- Recepción y registro de solicitudes de los funcionarios.
- Diagnóstico de la falla reportada (Software y Hardware)

[22] ICBF, PERFILES DE PRESTACION DE SERVICIO, EN LINEA. http://www.icbf.gov.co/portal/page/portal/PortalICBF/LeyTransparencia/EstudiosdeMercado/E2014/DInfoyTecnologia/Tab1/Redes%20-%20140828%20-%20ANEXO%206.5.6-PERFILES%20PROFESIONALES%20REQUERIDOS.pdf

- Realizar el procedimiento de atención de solicitudes tecnológicas de los funcionarios.
- Mantener actualizada la información relacionada con el licenciamiento del software del ICBF.
- Realizar gestión proactiva de problemas sobre los servicios contratados con el proveedor, reportando aquellos eventos a que al presentarse afecten o puedan afectar la continuidad en la operación.
- Cumplir a cabalidad y con estricto cumplimiento las labores de acompañar y reportar los resultados de las tareas masivas.
- Atender / Diagnosticar y solucionar los incidentes/requerimientos que son escalados por los agentes de la mesa de servicios.
- Velar por el buen funcionamiento de los recursos Informáticos y el cumplimiento de las políticas impartidas desde la Subdirección de Recursos Tecnológicos.

3.7 DESCRIPCIÓN DE ACTIVOS CRÍTICOS QUE DEBEN SEGUIR FUNCIONANDO.

A continuación se describen los activos críticos de la empresa, el cual son de uso principal para la continuidad de las actividades perteneciente a los procesos misionales.

- Personal: Empleados y contratistas.

- Hardware: Computadores, equipos de comunicaciones (Router, Switch, cableado).

- Software: Aplicaciones misional Web, sistema operativo.

- Auxiliares: UPS, Impresoras.

- Servicios: Procesos misionales (Información digital y física)

3.8 EVENTOS DE CONTINGENCIA.

Se consideran varias causas de interrupción por la cual suceden los eventos de contingencias, las cuales se tienen: Fallos de recursos tecnológicos, ausencia de personal, Difícil acceso al lugar de trabajo, corte de fluido eléctrico. Teniendo en cuenta esas interrupciones se presentan los siguientes eventos de contingencia. [16]

- **Contingencia por Ausencia de personal:**

Para esta contingencia se establecer la siguiente cadena de comunicación.

El funcionario ausente informa por Teléfono y se comunica con el Coordinador del Grupo de su área informando que no puede asistir a su trabajo.

- El Coordinador del Grupo informa ante el jefe del área que no puede asistir al trabajo el empleado e inmediatamente asignar las funciones a otra persona.
- Se informa a la oficina de sistemas para la creación de perfil al empleado suplente.
- El Coordinador del Grupo verifica la continuidad exitosa de los procesos.

- **Contingencia por fallas tecnológicas.**

Este tipo de contingencia se refiere cuando se presentan fallas en los sistemas informáticos, impidiendo la continuidad del servicio, estas fallas se

refieren a los procedimientos de solicitudes tecnológicas, se encuentran detallados en el anexo B.

3.8 DESCRIPCIÓN DE ACTIVIDAD PARA VOLVER A LA NORMALIDAD.

En la organización cuando una emergencia es superada, todas las actividades deben volver a la normalidad, a continuación se presenta los pasos del proceso indicando cuando los usuarios retornan a sus actividades laborales.

Tabla 28: Actividades para volver a la normalidad ante un desastre.

N	ACTIVIDAD	RESPONSABLES
1	Cuando el comité operativo de emergencias informa la solución del problema presentado, el funcionario responsable de la mesa de servicio identifica el último número de Radicación asignado en contingencia.	Brigadistas y mesa de servicios.
2	El coordinador del área informa a los funcionarios para que reanuden la Operativa.	Coordinador del área.
3	El coordinador del área firme el acta de atención a la emergencia indicando la atención inmediata y que fue superado en el tiempo indicado.	Coordinador del área.
4	Se anexa el acta a la herramienta de servicios y se cierra el caso.	Mesa de servicios.

Fuente: El autor.

ANEXO C

FOTOS DEL CUARTO DE COMUNICACIONES Y OFICIAS DEL CENTRO ZONAL.

CUARTO TECNICO DE CABLEADO

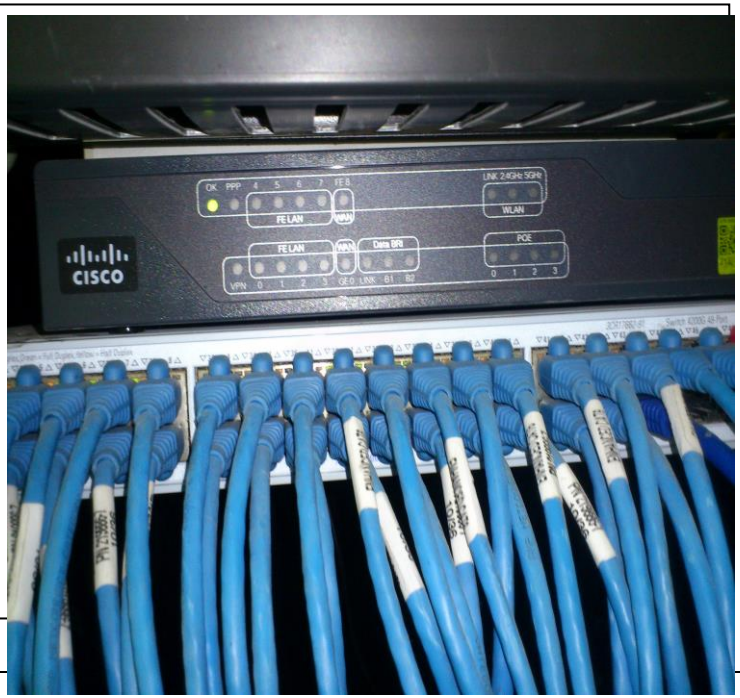
Rack de Comunicaciones

Rack principal de comunicaciones

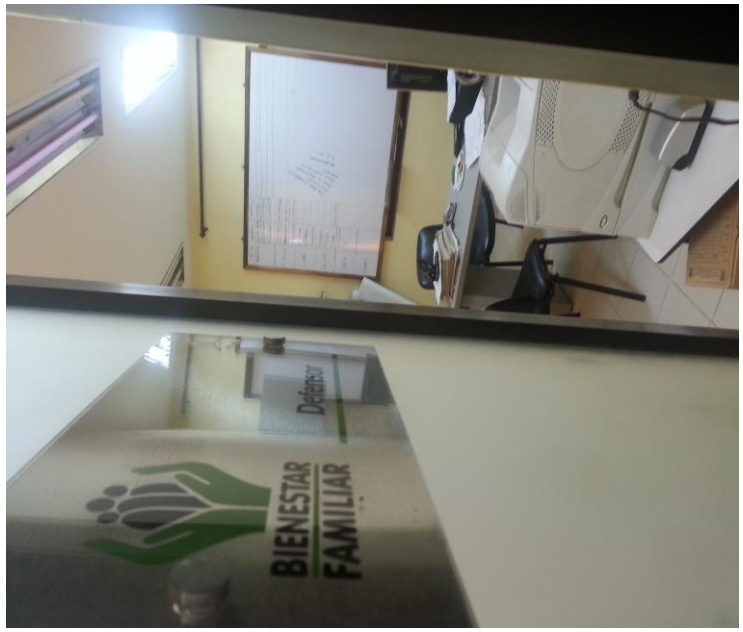
Fuente: El autor

EQUIPOS DE COMUNICACIONES

UPS



Fuente: El autor.

OFICINAS DEL ICBF	
	
Fuente: El autor	Fuente: El autor

Fuente: El autor

RESUMEN ANALITICO EDUCATIVO
RAE

Título del texto	**DISEÑAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA NORMA ISO 27001 EN EL INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR CENTRO ZONAL VIRGEN Y TURÍSTICO DE LA REGIONAL BOLIVAR**
Nombres y Apellidos del Autor	**Bueno Bustos Shirley Sandra**
Año de la publicación	**2016**

Resumen del texto: El ICBF Centro Zonal Virgen y Turístico Regional Bolívar ubicado en la Ciudad de Cartagena, no cuenta con suficiente normas de seguridad que ayuden a proteger los activos de información, esto ha originado que se presentan diferentes incidentes de seguridad tales como: la perdida de información, daño de equipos informáticos, borrado y modificación de información sensible, infiltración o acceso no autorizado en los sistemas, suplantación de personal, Craqueo de contraseñas, deterioro de activos físicos y dificultad en el acceso a los servicios por parte de terceros, entre otras.

Como respuesta a esta problemática se elabora el presente proyecto, el cual busca diseñar un sistema de gestión de seguridad de la información que permita conocer las vulnerabilidades, amenazas y riesgos a los cuales están expuestos los activos, para así establecer objetivos, políticas, procedimientos y acciones encaminadas a garantizar la confidencialidad, disponibilidad e integridad de los activos de información que tiene la empresa, y de igual forma mantener el nivel de riesgo en un nivel aceptable.

Palabras Claves:	ISO 27001, SGSI, Vulnerabilidad, Activos de Información, MAGERIT, Gestión de Riesgo, Políticas de seguridad, Seguridad de la Información, Amenazas, Riesgo, Confidencialidad, Integridad, Disponibilidad.

Problema que aborda el texto: Los problemas de seguridad en las empresas son originados por la explotación de vulnerabilidades en los activos de información, ausencia de controles y procedimientos mal definidos. En el ICBF Centro Zonal Virgen y Turístico, existen aamenazas que

diariamente afectan a los activos, entre las más destacables podemos mencionar: La pérdida de integridad de información digital, infiltración o acceso no autorizado en los sistemas, propagación de virus y software malicioso, suplantación de personal, uso de contraseñas débiles, deterioro de activos físicos, perdida de documentos, fallas de hardware, problemas de recuperación de información, perdida de documentos físicos, fallas en el Hardware, problemas de recuperación de información, problemas de denegación de servicios, problemas con ubicación en áreas susceptibles a desastres, divulgación de información, información oculta en las memorias USB, equipos dañados, entre otros.

Objetivos del texto:

OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información utilizando la norma ISO 27001:2013 en el ICBF Centro Zonal Virgen y Turístico, Regional Bolívar.

OBJETIVOS ESPECIFICOS.

Identificar las vulnerabilidades que afectan los activos del ICBF centro zonal Virgen y Turístico Regional Bolívar.

Identificar las amenazas de seguridad informática que afectan los activos de la organización mediante un análisis de vulnerabilidades.

Establecer los procedimientos documentados de manera sistemática usando norma ISO 27001 que permitan minimizar los riesgos de seguridad.

Establecer los objetivos de control a implementar para la eficacia del SGSI en el ICBF centro zonal virgen y Turístico regional Bolívar.

Definir las políticas de seguridad informática que se deben implementar en la entidad basada en la norma ISO 27001.

Conclusiones del texto: El presente proyecto cumplió todos los objetivos y se logró diseñar el sistema de gestión de seguridad de la información para el ICBF, Centro Zonal Virgen y Turístico, Regional Bolívar. Al finalizar el presente proyecto se obtuvieron las siguientes conclusiones:

- Se identificaron los activos de información con su respectivo inventario.
- Se identificaron todas las vulnerabilidades y amenazas en la empresa, realizando un listado con su respectiva valoración del estado actual de los activos.
- Se realizó la gestión de riesgos utilizando la metodología MAGERIT, identificando los riesgos de mayor afectación para la empresa de acuerdo a los resultados del nivel de valoración.
- Se identificaron los riesgos altos, muy altos y críticos y se realizó el tratamiento adecuado para cada uno de ellos.
- Se establecieron los objetivos de control y controles para cada riesgo encontrado al interior del ICBF.
- Se documentaron las políticas de seguridad que se deben aplicar para la protección debida de los activos.
- Se realizaron los procedimientos de Backup, procedimientos de copia de seguridad, procedimiento de soporte técnico.
- Con el desarrollo de este proyecto se espera que la empresa implemente los controles y medidas que permitan lograr un nivel aceptable de seguridad.

Metodología

LINEA DE INVESTIGACIÓN: Teniendo en cuenta las líneas de investigación ofrecida por la escuela ECBTI (Escuela de Ciencias Básica, Tecnología e Ingenierías), para el desarrollo de este proyecto

se aplicará **LA LÍNEA DE GESTIÓN DE SISTEMAS DEL ÁREA DE LA CIENCIAS DE LA COMPUTACIÓN**, el cual según Salazar (1999), está orientada a integrar, planificar y controlar los aspectos técnicos, humanos, organizativos, comerciales y sociales del proceso completo, empezando con el análisis del dominio del problema, continuando con el diseño de alternativas de solución y finalizando con la operatividad de un sistema. La idea de esta línea es que a partir conceptualización se pueda evaluar la situación actual y las perspectivas de los procesos para hacerlos más eficientes y dinámicos, a partir de la investigación aplicada, impulsada por la investigación inductiva y participativa.

Los pasos a seguir en la investigación serán tomados en la siguiente manera:

- Definir el alcance del SGSI en cuanto al objetivo de la empresa, su localización, sus activos y tecnología.
- Definir una política de seguridad que incluya el marco general y los objetivos de seguridad de la información de la organización.
- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del riesgo, para este proyecto se usara la metodología MAGERIT, su objetivo es identificar los riesgos de información que tiene la empresa, realizando la identificación de los activos, análisis de vulnerabilidades, amenazas y la identificación de los objetivos de control a implementar para disminuir esos riesgos.

- Realizar el análisis y evaluación de riesgos, evaluar los impactos en los activos cuando ocurre una amenaza y los niveles de riesgos.

- Identificar y evaluar las distintas opciones de tratamiento de los riesgos aplicando los controles adecuados.

Bibliografía citada por el autor:

RAMIREZ VILLEGAS, G. M., & CONSTAIN MORENO, G. E. (2012). Modelos y Estandares de Seguridad Informatica. Palmira.

ROZO, E. A. (Enero de 2013). PROYECTO DE SEGURIDAD INFORMÁTICA I. La Plata, Huila,

Colombia.

PORTAL DE ISO 27001 EN ESPAÑOL, 28 de Agosto del 2015, [En línea] http://www.iso27000.es/download/doc_sgsi_all.pdf.

ACADEMY, QUE ES LA ISO 27001. Tomado el día 29 de Agosto. [En línea] http://advisera.com/27001academy/es/que-es-iso-27001/.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, Tomado el día 29 de Agosto del 2015, [En línea]. http://www.iso27000.es/download/doc_sgsi_all.pdf.

QUINTERO JOSE LUIS ANALISIS Y GESTIÓN DEL RIESGO. Tomado el día 30 de Agosto del 2015, [En línea] http://www.aec.es/c/document_library/get_file?uuid=b3945e58-17f2-4dc0-88ac-863ae9f998cb&groupId=10128.

ISO 27001, ORIGEN E HISTORIA. Tomado el día 31 de Agosto del 2015. [En línea] http://www.pmg-ssi.com/2013/12/iso27001-origen/

HALABY WILLIAM, CAMBIOS RESPECTO A ISO 27001:2013, CHARTER COLOMBIA. Tomado el día 31 de Agosto del 2015. [En línea]. http://isc2capitulocolombia.org/portal/images/documents/ISO_27001-2013_ISC2_Colombia_Chapter.pdf

CORPORACION COLOMBIA DIGITAL, LEY DE PROTECCION DE DATOS PERSONALES: Una Realidad en Colombia. Tomado el día 1 de Setiembre del 2016.

POVEDA JOSE MANUEL, Activos de Seguridad de la Información, Modulo 7, ISO 27001. Tomado el día 24 de Julio del 2015. [En línea]. http://www.worldvisioncapacitacion.cl/wp-content/uploads/cursos_adjuntos/f52e0bd4c6c2c203413952826f916237.pdf

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS, Oficina Asesora de Sistemas, Gestión del Riesgo, Capitulo 8, 10 de Agosto del 2015. [En línea] http://www.udistrital.edu.co:8080/documents/276352/356568/Cap5GESTIÓN Riesgo.pdf

BOLAÑOS, MARÍA C y ROCHA G. MONICA. 15 de Julio del 2015. MAGERIT V 3.0, (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). [En línea] http://es.slideshare.net/kinny32/magerit-v3-libro1metodo.

POVEDA JOSE MANUEL, Análisis y Valoración de los Riesgos, Modulo 8, ISO 27001. 30 de Julio del 2015. [En línea]. https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

BERNAL JIMENO JORGE, 20 de Agosto del 2015, CICLO PHCA (Planificar, Hacer, Verificar, Actuar): el circulo Deming de mejora continua (En línea) http://www.pdcahome.com/5202/ciclo-pdca.

MARCO LEGAL DE LA SEGURIDAD INFORMATICA EN COLOMBIA (línea) Disponible en: http://seguridadinformacióncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html

PORTAL WEB INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR, 20 de septiembre del 2014. (En línea), Disponible en: http:// www.icbf.gov.co.

FERRER RODRIGO, Sistema de Gestión de Seguridad de la Información. (En linea). Sisteseg.com: http://www.sisteseg.com/files/Microsoft_PowerPoint_-_Estrategias_de_seguridad_v52.pdf

ICBF, PROCEDIMIENTO DE GESTIÓN DE BACKUP, [en línea]. http://www.icbf.gov.co/portal/page/portal/IntranetICBF/macro_procesos/MP_apoyo/GESTIÓN_tecnologica/PR11-MPA6-GESTIÓN -Copias-de-Seguridad-v2_1.pdf

Nombre y apellidos de quien elaboró este RAE	**SHIRLEY SANDRA BUENO BUSTOS**
Fecha en que se elaboró este RAE	18/04/2016
Comentarios finales:	