PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

INDEPORTES ANTIOQUIA

INTRODUCCIÓN

La estrategia de Gobierno Digital en Colombia se enmarca en la construcción de un Estado más eficiente, transparente y participativo, que, con el apoyo de las tecnologías de la información y las comunicaciones, refleja un desarrollo sobre la base de los siguientes cuatro ejes temáticos: TIC para el estado, TIC para la sociedad y habilitadores transversales. Atendiendo lo expuesto, el Ministerio de las Tecnologías de la Información y las Comunicaciones, ha definido el Modelo de Seguridad y Privacidad de la Información, denominado MSPI, como un componente transversal basado en la adopción de mejores prácticas y metodologías como: la norma ISO/IEC 27001:2013, ITIL, COBIT, entre otras.

En INDEPORTES ANTIOQUIA, se han venido adelantando una serie de actividades, cuyo propósito es cumplir con las metas definidas en el MSPI y se centra en la implementación de un Sistema de Gestión de Seguridad de la Información – SGSI, basado en la norma ISO 27001:2013. Relacionadas con el diagnóstico de seguridad de la información para el proceso de Direccionamiento, con el fin de determinar las brechas existentes respecto al cumplimiento de la norma ISO 27001:2013, la identificación, clasificación y valoración de los activos de información, así como el análisis de riesgos de los activos, del que hacen parte la gerencia general, y las demás dependencias, de acuerdo con el mapa institucional de procesos.

TABLA DE CONTENIDO

INTRODUCCIÓN 2

ORGANIGRAMA 4

MAPA DE PROCESOS 5

OBJETIVO GENERAL 6

OBJETIVOs especificos 6

PILARES 7

METODOLOGÍA 8

ACTIVOS Y AMENAZAS 10

TABLAS VALORACIÒN 11

ESCENARIO DE RIESGOS 12

AGENTE GENERADOR 13

VALORACIÓN DEL RIESGO 19

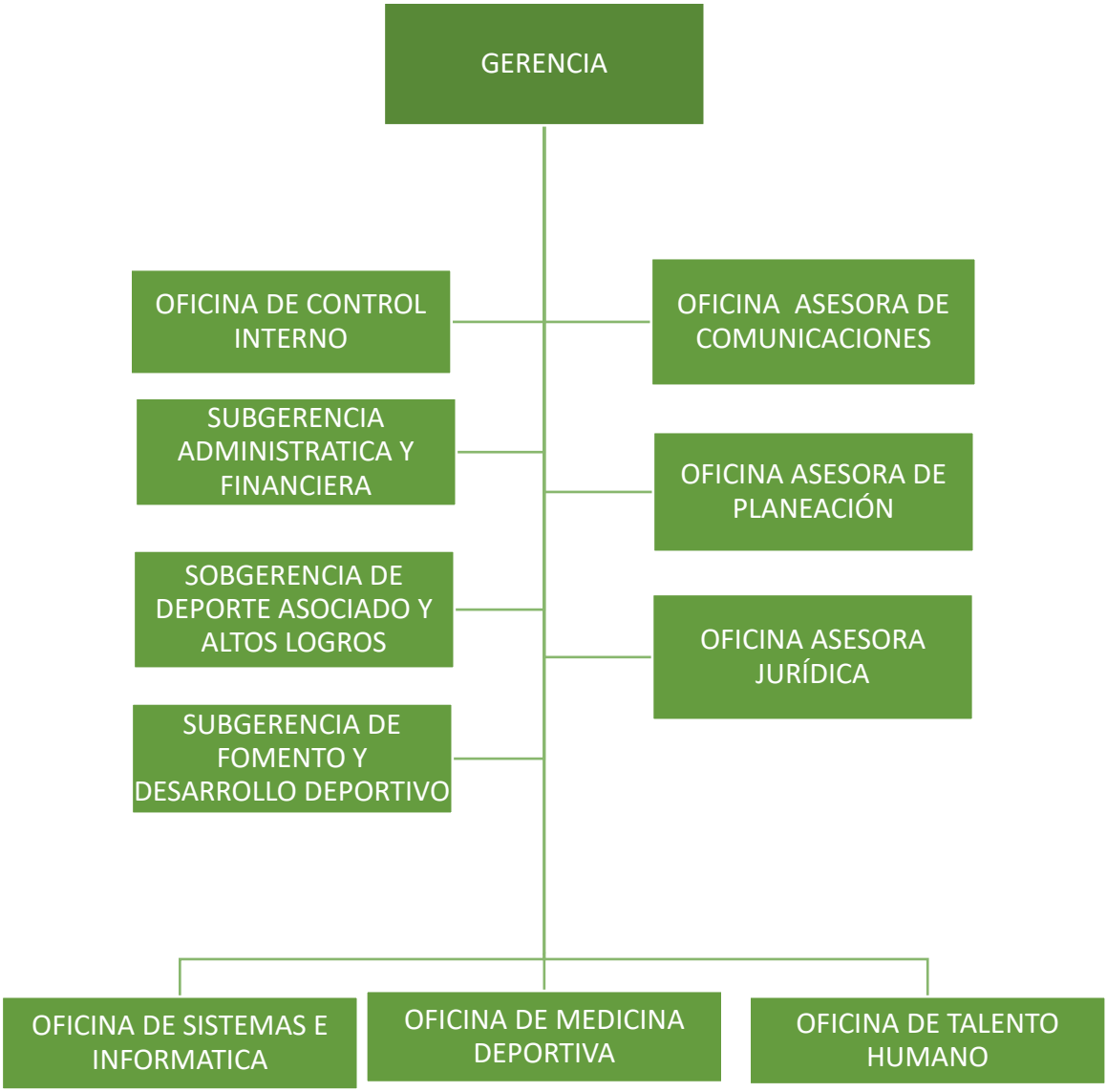
PLAN CULTURAL 22

MEDICIÓN DE CONTROLES 27

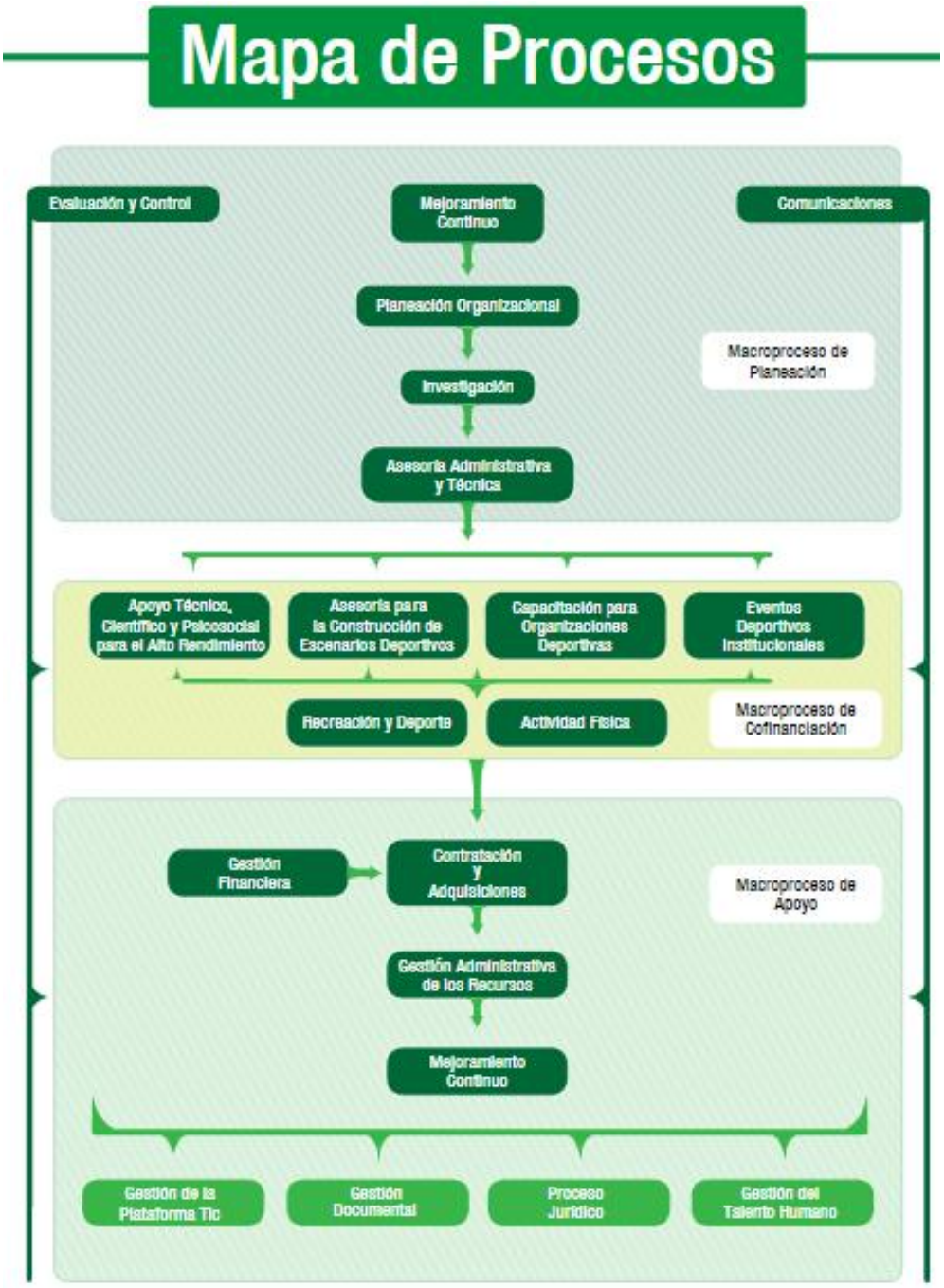
CONCLUSIONES 28

SEGUIMIENTO 28

ORGANIGRAMA



MAPA DE PROCESOS



OBJETIVO GENERAL

Realizar el análisis de brecha, identificación y evaluación de riesgos de los activos de información del proceso de Direccionamiento de INDEPORTES ANTIOQUIA, para asegurar que los riesgos sean conocidos y gestionados adecuadamente por parte de los usuarios responsables de la información con el fin de proteger la información contra una gran variedad de amenazas, minimizando el riesgo y asegurando la continuidad del servicio, acorde a los lineamientos definidos por el Departamento Administrativo de la Función Pública, el Ministerio de las TIC y el programa de Gobierno Digital

OBJETIVOS ESPECIFICOS

- Establecer el nivel de cumplimiento del proceso de Direccionamiento frente a los objetivos de control y controles establecidos en el Anexo A de la ISO 27001:2013.

- Identificar, valorar y clasificar los activos de información del proceso de Direccionamiento de INDEPORTES ANTIOQUIA.

- Realizar el análisis de riesgos de seguridad de la información, tomando como referencia la metodología de gestión del riesgo que utiliza la entidad.

- Elaborar la declaración de aplicabilidad y definir el plan de tratamiento de los riesgos identificados y evaluados.

PILARES

Los pilares fundamentales del Plan de Tratamiento de Riesgo de Seguridad de la Información en el Instituto son los definidos por la norma ISO27001:2013, Integridad, Disponibilidad y Confidencialidad de la información:

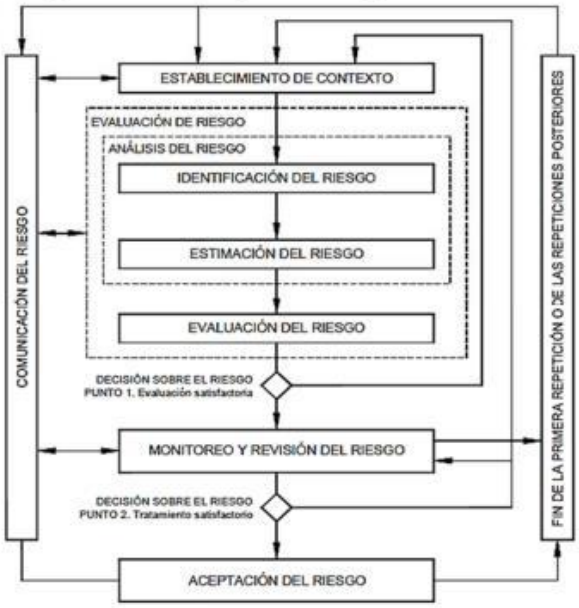
Integridad: Aseguramiento de no alteración de datos. La integridad de los datos es tener la seguridad de que la información no se ha alterado en la transmisión, desde el origen hasta la recepción.

Confidencialidad: Asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.

Disponibilidad: Aseguramiento de que los autorizados tengan acceso cuando lo necesiten a la información y a los activos asociados.

METODOLOGÍA

Proceso de gestión del riesgo en la seguridad de la información.



Fuente: NTC-ISO 27005

El análisis de riesgo aplicado a los activos de información permite comprender los riesgos sobre los activos de información a los que puede estar expuesto INDEPORTES ANTIOQUIA.

En un SGSI, el establecimiento del contexto, la valoración del riesgo, el desarrollo del plan de tratamiento del riesgo y la aceptación del riesgo son parte de la fase de "planificar". En la fase de "hacer" del SGSI, se implementan las acciones y los controles que son necesarios para reducir el riesgo hasta un nivel aceptable, de acuerdo con el plan de tratamiento del riesgo.

En la fase de "verificar" del SGSI, la dirección determinará la necesidad de revisiones de las valoraciones y del tratamiento del riesgo a la luz de los incidentes y los cambios en las circunstancias.

En la fase de "actuar", se llevan a cabo todas las acciones que son necesarias, incluyendo la aplicación adicional del proceso de gestión del riesgo en la seguridad de la información. Dentro del ciclo PHVA, la evaluación de riesgos de la seguridad de la información requiere adelantar una serie de actividades, las cuales de manera general se pueden apreciar en las siguientes tablas:

Tabla 5. Dominios de la norma NTC-ISO 27001:2013

Dominio ISO 27001	Objetivo de Control
Política de seguridad	Objetivo de control A.5
Organización de la seguridad de la información	Objetivo de control A.6
Seguridad de los RRHH	Objetivo de control A.7
Gestión de activos	Objetivo de control A.8
Control de acceso	Objetivo de control A.9
Criptografía	Objetivo de control A.10
Seguridad física y ambiental	Objetivo de control A.11
Seguridad en la operaciones	Objetivo de control A. 12
Seguridad en las comunicaciones	Objetivo de control A.13
Adquisición de sistemas, desarrollo y mantenimiento	Objetivo de control A.14
Relación con proveedores	Objetivo de control A.15
Gestión de los incidentes de seguridad	Objetivo de control A.16
Continuidad de negocio	Objetivo de control A.17
Cumplimiento con requerimientos legales y contractuales	Objetivo de control A.18

Fuente: Manual del SGSI

Tabla 6. Nivel de madurez – MSPI

Nivel	Porcentaje	Criterios
Inexistente	0%	No se cuenta con la cláusula o control. No se reconoce la información como un activo importante para el logro de la misión y visión de la entidad.
Inicial	1-20%	El control esta implementado no obstante el modelo de seguridad de políticas, procedimientos y estándares de configuración, no existe.
Repetible	21-40%	El control esta implementado y además es soportado por un documento que contiene una política de alto nivel y otras políticas operativas debidamente aprobadas.
Definido	41-60%	El control esta implementado y soportado por políticas, procedimientos y estándares de configuración debidamente publicados y socializados.
Administrado	61-80%	En este nivel se realizan mediciones sobre la efectividad de los controles.
Optimizado	81-100%	En este nivel se encuentran las entidades en las cuales se mide la efectividad de los controles con el fin de mejorarlos y optimizarlos.

Fuente: Modelo de seguridad y privacidad de la información

ACTIVOS Y AMENAZAS

ACTIVOS	
TANGIBLES	Routes
	Swiches
	Estaciones de trabajo
	Acces Point
	Dispositivos moviles y electronicos
	Control de acceso ingreso
	Cableado Estructurado
	UPS
	Impresoras y Scaner
	Sistema de camaras vigilancia
INTANGIBLES	Servidores Virtuales
	Servidores correo,archivos, web
	Bases de Datos
	Sistemas de Informacion
	Controlador de dominio Directorio Activo
	Informacion
	Licencias

AMENAZAS TIC	AMENAZAS NATURALES	AMENAZAS HUMANAS/SOCIALES
Suplantacion de identidad	Incendios	Atentados terroristas
Virus-malware	Terremotos	Manifestaciones
Robo de información	Tormentas eléctricas	Orden Publico
Robo de infraestructura	Inundaciones	
SQL Injection	Alud	
Alteración maliciosa de la información		
Sniffers		
Denegacion de servicios		
Conexiones no autorizadas		
Spammer		
Ingenieria social		
ex-empleados o empleados insatisfechos		

TABLAS VALORACIÒN

TABLAS DE PROBABILIDAD/FRECUENCIA(ocurrencia)			
Nivel	Rangos	Ejemplo detallado de la descripción	
1	Muy ocasional	Puede ocurrir solo bajo circunstancias excepcionales	1 vez cada 5 años
2	Ocasional	Podría ocurrir algunas veces	1 vez por año
3	Posible	Puede ocurrir en algún momento	1 vez cada 6 meses
4	Casi seguro	La expectativa de ocurrencia se da forma periodica	1 vez por mes
5	Muy seguro	La expectativa de ocurrencia se da en la mayoría de circunstancias	3 veces por semana

Impacto en la OPERACIÓN		
Nivel	Rangos	Ejemplo detallado de la descripción
1	Insignificante	Hay una indisponibilidad menor a 4 horas y la puede resolver equipo de soporte tecnico.
2	Menor	Hay una indisponibilidad entre 12 hora, es necesario escalarlo a 2 nivel
3	Medio	Hay una indisponibilidad entre 12 a 24 horas, se requiere consulta con terceros (proveedor)
4	Mayor	Hay una indisponibilidad entre 24 a 48 horas, utilizamos otro mecanismo
5	Superior	Hay una indisponibilidad por más de 48 horas, es necesario establecer un mecanismo de procesamiento alterno, o, se ha perdido loa confidencialida.

Impacto en la INFORMACIÓN (disponibilidad, confiabilidad, integridad)				
Nivel	Rangos	Ejemplo detallado de la descripción-disponibilidad	Confiabilidad	
1	Insignificante	La información no esta disponible por menos de 3 horas.	La información puede ser porcesada sin retrazos en los proyectos/procesos.	Hay una disponibilidad menor a 4 horas y la puede resolver equipo de soporte tecnico.
2	Menor	La información no esta disponible 3 y 8 horas		Hay una disponibilidad entre 12 hora, es necesario escalarlo a 2 nivel
3	Medio	La información no esta disponible 8 y 14 horas		Hay una disponibilidad entre 12 a 24 horas, se requiere consulta con terceros (proveedor)
4	Mayor	La información no esta disponible entre 14 y de 24 horas		Hay una disponibilidad entre 24 a 48 horas, utilizamos otro mecanismo
5	Superior	La información no esta disponible por más de 24 horas	La información confiabilidad de la información afecta considerablemente al negocio. No hay fiabilidad de los datos.	Hay una disponibilidad por más de 48 horas, es necesario establecer un mecanismo de procesamiento alterno o se ha perdido la confidencialidad.

Impacto en la IMAGEN		
Nivel	Rangos	Ejemplo detallado de la descripción
1	Insignificante	Se identifica el problema de imagen a nivel del grupo de trabajo.
2	Menor	Se identifica el problema de imagen a nivel Sede
3	Medio	Se identifica el problema de imagen a nivel empresa.
4	Mayor	Se identifica el problema de imagen a nivel regional.
5	Superior	Se identifica el problema de imagen a nivel nacional.

ESCENARIO DE RIESGOS

AMENAZAS/ACTIVOS	Routes	Swiches	Estaciones de trabajo	Acces Point	Dispositivos moviles y electronicos	Control de acceso ingreso	Cableado estructurado	UPS	Impresoras y Scaner	Sistema de camaras vigilancia	Servidores Virtuales	Servidores correo,archivos, web	Bases de Datos	Sistemas de Informacion	Controlador de dominio Directorio Activo	Informacion	Licencias
Suplantacion de identidad			X								X	X				X	
Virus-malware	X	X	X	X	X		X		X	X	X	X	X	X	X	X	X
Robo de información o (Ransomware)			X		X		X			X	X	X	X	X		X	X
Robo de infraestructura	X	X	X	X	X	X	X	X	X	X					X		
SQL Injection (bases de datos)											X	X	X			X	
Alteración maliciosa de la información			X						X	X	X	X		X	X	X	X
Sniffers (trafico de datos)	X	X		X			X			X	X		X				
Denegacion de servicios		X	X							X	X	X	X	X	X	X	
Conexiones o accesos no autorizadas	X	X	X	X			X		X	X	X	X	X	X		X	
Spammer			X									X				X	
Ingenieria social			X		X		X		X	X	X		X	X	X	X	X
ex-empleados o empleados insatisfechos			X		X	X	X	X	X	X				X	X	X	X
Incendios	X	X	X	X	X	X	X	X	X	X		X			X		
Terremotos	X	X	X	X	X	X	X	X	X	X		X		X	X		
Tormentas eléctricas	X	X	X	X	X		X	X	X	X		X		X	X		
Inundaciones	X	X	X	X	X	X	X	X	X			X		X	X		
Alud	X	X	X	X	X	X	X	X	X	X		X		X	X		
Atentados terroristas	X	X	X	X	X	X	X	X	X	X		X	X	X	X		
Manifestaciones	X	X	X	X	X	X	X	X	X	X		X		X	X		
Orden Público			X	X	X	X	X	X	X	X							

AGENTE GENERADOR

Escenario del riesgos	Agente Generador	Causa	Efecto
Suplantacion de identidad -- Estaciones de trabajo	Ataque	Vulnerabilidad	Fuga de Información
Suplantacion de identidad -- Servidores Virtuales	Ataque	Vulnerabilidad	Robo de informacion
Suplantacion de identidad -- Servidores correo,archivos, web	Ataque	Vulnerabilidad	Ataques a través de paquetes (SPAM)
Suplantacion de identidad -- Informacion	Ataque	Vulnerabilidad	Robo de informacion
Virus-malware -- Routes	Ataque	Vulnerabilidad	Daño-Alteración de la Información
Virus-malware -- Swiches	Ataque	Vulnerabilidad	Daño-Alteración de la Información
Virus-malware -- Estaciones de trabajo	Ataque	Vulnerabilidad	Robo de informacion
Virus-malware -- Acces Point	Ataque	Vulnerabilidad	Robo de informacion
Virus-malware -- Dispositivos moviles y electronicos	Ataque	Vulnerabilidad	Robo de informacion
Virus-malware -- Cableado estructurado	Ataque	Vulnerabilidad	Daño-Alteración de la Información
Virus-malware -- Impresoras y Scaner	Ataque	Vulnerabilidad	Robo de informacion
Virus-malware -- Sistema de camaras vigilancia	Ataque	Vulnerabilidad	Daño-Alteración de la Información
Virus-malware -- Servidores Virtuales	Ataque	Vulnerabilidad	Daño-Alteración de la Información
Virus-malware -- Servidores correo,archivos, web	Ataque	Vulnerabilidad	Robo de informacion
Virus-malware -- Bases de Datos	Ataque	Vulnerabilidad	Robo de informacion
Virus-malware -- Sistemas de Informacion	Ataque	Vulnerabilidad	Daño-Alteración de la Información
Virus-malware -- Controlador de dominio Directorio Activo	Ataque	Vulnerabilidad	Daño-Alteración de la Información
Virus-malware -- Informacion	Ataque	Vulnerabilidad	Robo de informacion
Virus-malware -- Licencias	Ataque	Vulnerabilidad	Robo de informacion
Robo de información o (Ransomware) -- Estaciones de trabajo	Software malicioso	Vulnerabilidad	Daño y pérdida de la Información
Robo de información o (Ransomware) -- Dispositivos moviles y electronicos	Software malicioso	Vulnerabilidad	Daño y pérdida de la Información
Robo de información o (Ransomware) -- Cableado estructurado	Software malicioso	Vulnerabilidad	Daño y pérdida de la Información
Robo de información o (Ransomware) -- Sistema de camaras vigilancia	Software malicioso	Vulnerabilidad	Daño y pérdida de la Información
Robo de información o (Ransomware) -- Servidores Virtuales	Software malicioso	Vulnerabilidad	Daño y pérdida de la Información
Robo de información o (Ransomware) -- Servidores correo,archivos, web	Software malicioso	Vulnerabilidad	Daño y pérdida de la Información
Robo de información o (Ransomware) -- Bases de Datos	Software malicioso	Vulnerabilidad	Daño y pérdida de la Información
Robo de información o (Ransomware) -- Sistemas de Informacion	Software malicioso	Vulnerabilidad	Daño y pérdida de la Información
Robo de información o (Ransomware) -- Informacion	Software malicioso	Vulnerabilidad	Robo de informacion
Robo de información o (Ransomware) -- Licencias	Software malicioso	Vulnerabilidad	Robo de informacion
Robo de infraestructura -- Routes	Delincuencia	Debilidad en la Seguridad Física	indisponibilidad de la Información
Robo de infraestructura -- Swiches	Delincuencia	Debilidad en la Seguridad Física	indisponibilidad de la Información
Robo de infraestructura -- Estaciones de trabajo	Delincuencia	Debilidad en la Seguridad Física	indisponibilidad de la Información
Robo de infraestructura -- Acces Point	Delincuencia	Debilidad en la Seguridad Física	indisponibilidad de la Información
Robo de infraestructura -- Dispositivos moviles y electronicos	Delincuencia	Debilidad en la Seguridad Física	indisponibilidad de la Información
Robo de infraestructura -- Control de acceso ingreso	Delincuencia	Debilidad en la Seguridad Física	indisponibilidad de la Información
Robo de infraestructura -- Cableado estructurado	Delincuencia	Debilidad en la Seguridad Física	indisponibilidad
Robo de infraestructura -- UPS	Delincuencia	Debilidad en la Seguridad Física	indisponibilidad
Robo de infraestructura -- Impresoras y Scaner	Delincuencia	Debilidad en la Seguridad Física	indisponibilidad de la Información
Robo de infraestructura -- Sistema de camaras vigilancia	Delincuencia	Debilidad en la Seguridad Física	indisponibilidad de la Información
Robo de infraestructura -- Controlador de dominio Directorio Activo	Delincuencia	Debilidad en la Seguridad Física	indisponibilidad de la Información
SQL Injection (bases de datos) -- Servidores Virtuales	Código intruso	Vulnerabilidad	Infiltración en la Información
SQL Injection (bases de datos) -- Servidores correo,archivos, web	Código intruso	Vulnerabilidad	Infiltración en la Información
SQL Injection (bases de datos) -- Bases de Datos	Código intruso	Vulnerabilidad	Infiltración en la Información
SQL Injection (bases de datos) -- Informacion	Código intruso	Vulnerabilidad	Infiltración en la Información
Alteración maliciosa de la información -- Estaciones de trabajo	Malware	Vulnerabilidad	Alteración de la Información
Alteración maliciosa de la información -- Impresoras y Scaner	Malware	Vulnerabilidad	Alteración de la Información
Alteración maliciosa de la información -- Sistema de camaras vigilancia	Malware	Vulnerabilidad	Alteración de la Información
Alteración maliciosa de la información -- Servidores Virtuales	Malware	Vulnerabilidad	Alteración de la Información
Alteración maliciosa de la información -- Servidores correo,archivos, web	Malware	Vulnerabilidad	Alteración de la Información
Alteración maliciosa de la información -- Sistemas de Informacion	Malware	Vulnerabilidad	Alteración de la Información
Alteración maliciosa de la información -- Controlador de dominio Directorio Activo	Malware	Vulnerabilidad	Alteración de la Información
Alteración maliciosa de la información -- Informacion	Malware	Vulnerabilidad	Alteración de la Información
Alteración maliciosa de la información -- Licencias	Malware	Vulnerabilidad	Alteración de la Información
Sniffers (trafico de datos) -- Routes	Ataques	Amenaza	Daños y Robo de Información
Sniffers (trafico de datos) -- Swiches	Ataques	Amenaza	Daños y Robo de Información
Sniffers (trafico de datos) -- Acces Point	Ataques	Amenaza	Daños y Robo de Información
Sniffers (trafico de datos) -- Cableado estructurado	Ataques	Amenaza	Daños y Robo de Información
Sniffers (trafico de datos) -- Sistema de camaras vigilancia	Ataques	Amenaza	Daños y Robo de Información
Sniffers (trafico de datos) -- Servidores Virtuales	Ataques	Amenaza	Daños y Robo de Información
Sniffers (trafico de datos) -- Bases de Datos	Ataques	Amenaza	Daños y Robo de Información
Denegacion de servicios -- Swiches	Ataques	Débil configuración control de seguridad	Indisponibilidad de la Información
Denegacion de servicios -- Estaciones de trabajo	Ataques	Débil configuración control de seguridad	Indisponibilidad de la Información
Denegacion de servicios -- Sistema de camaras vigilancia	Ataques	Débil configuración control de seguridad	Indisponibilidad de la Información
Denegacion de servicios -- Servidores Virtuales	Ataques	Débil configuración control de seguridad	Indisponibilidad de la Información
Denegacion de servicios -- Servidores correo,archivos, web	Ataques	Débil configuración control de seguridad	Indisponibilidad de la Información
Denegacion de servicios -- Bases de Datos	Ataques	Débil configuración control de seguridad	Indisponibilidad de la Información
Denegacion de servicios -- Sistemas de Informacion	Ataques	Débil configuración control de seguridad	Indisponibilidad de la Información
Denegacion de servicios -- Controlador de dominio Directorio Activo	Ataques	Débil configuración control de seguridad	Indisponibilidad de la Información
Denegacion de servicios -- Informacion	Ataques	Débil configuración control de seguridad	Indisponibilidad de la Información
Conexiones o accesos no autorizadas -- Routes	Personal Interno y externo de la empresa	Bajo nivel de control seguridad	Robo de Información
Conexiones o accesos no autorizadas -- Swiches	Personal Interno y externo de la empresa	Bajo nivel de control seguridad	Robo de Información
Conexiones o accesos no autorizadas -- Estaciones de trabajo	Personal Interno y externo de la empresa	Bajo nivel de control seguridad	Robo de Información
Conexiones o accesos no autorizadas -- Acces Point	Personal Interno y externo de la empresa	Bajo nivel de control seguridad	Robo de Información
Conexiones o accesos no autorizadas -- Cableado estructurado	Personal Interno y externo de la empresa	Bajo nivel de control seguridad	Robo de Información
Conexiones o accesos no autorizadas -- Impresoras y Scaner	Personal Interno y externo de la empresa	Bajo nivel de control seguridad	Robo de Información
Conexiones o accesos no autorizadas -- Sistema de camaras vigilancia	Personal Interno y externo de la empresa	Bajo nivel de control seguridad	Robo de Información
Conexiones o accesos no autorizadas -- Servidores Virtuales	Personal Interno y externo de la empresa	Bajo nivel de control seguridad	Robo de Información
Conexiones o accesos no autorizadas -- Servidores correo,archivos, web	Personal Interno y externo de la empresa	Bajo nivel de control seguridad	Robo de Información
Conexiones o accesos no autorizadas -- Bases de Datos	Personal Interno y externo de la empresa	Bajo nivel de control seguridad	Robo de Información
Conexiones o accesos no autorizadas -- Sistemas de Informacion	Personal Interno y externo de la empresa	Bajo nivel de control seguridad	Robo de Información
Conexiones o accesos no autorizadas -- Informacion	Personal Interno y externo de la empresa	Bajo nivel de control seguridad	Robo de Información
Spammer -- Estaciones de trabajo	Virus	Vulnerabilidad	Robo de Informacion
Spammer -- Servidores correo,archivos, web	Virus	Vulnerabilidad	Robo de Informacion
Spammer -- Informacion	Virus	Vulnerabilidad	Robo de Informacion
Ingenieria social -- Estaciones de trabajo	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y fuga de Informacion
Ingenieria social -- Dispositivos moviles y electronicos	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y fuga de Informacion
Ingenieria social -- Cableado estructurado	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y fuga de Informacion
Ingenieria social -- Impresoras y Scaner	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y fuga de Informacion
Ingenieria social -- Sistema de camaras vigilancia	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y fuga de Informacion
Ingenieria social -- Servidores Virtuales	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y fuga de Informacion
Ingenieria social -- Bases de Datos	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y fuga de Informacion

Ingenieria social -- Sistemas de Informacion	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y fuga de Informacion
Ingenieria social -- Controlador de dominio Directorio Activo	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y fuga de Informacion
Ingenieria social -- Informacion	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y fuga de Informacion
Ingenieria social -- Licencias	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y fuga de Informacion
ex-empleados o empleados insatisfechos -- Estaciones de trabajo	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y daño de Información
ex-empleados o empleados insatisfechos -- Dispositivos moviles y electronicos	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y daño de Información
ex-empleados o empleados insatisfechos -- Control de acceso ingreso	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y daño de Información
ex-empleados o empleados insatisfechos -- Cableado estructurado	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y daño de Información
ex-empleados o empleados insatisfechos -- UPS	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y daño de Información
ex-empleados o empleados insatisfechos -- Impresoras y Scaner	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y daño de Información
ex-empleados o empleados insatisfechos -- Sistema de camaras vigilancia	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y daño de Información
ex-empleados o empleados insatisfechos -- Sistemas de Informacion	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y daño de Información
ex-empleados o empleados insatisfechos -- Controlador de dominio Directorio Activo	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y daño de Información
ex-empleados o empleados insatisfechos -- Informacion	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y daño de Información
ex-empleados o empleados insatisfechos -- Licencias	Personal Interno y externo de la empresa	Bajo nivel de control	Robo y daño de Información
Incendios -- Routes	Desastres naturales o intencionales	Vulnerabilidad	Daños y Perdida de la Información
Incendios -- Swiches	Desastres naturales o intencionales	Vulnerabilidad	Daños y Perdida de la Información
Incendios -- Estaciones de trabajo	Desastres naturales o intencionales	Vulnerabilidad	Daños y Perdida de la Información
Incendios -- Acces Point	Desastres naturales o intencionales	Vulnerabilidad	Daños y Perdida de la Información
Incendios -- Dispositivos moviles y electronicos	Desastres naturales o intencionales	Vulnerabilidad	Daños y Perdida de la Información
Incendios -- Control de acceso ingreso	Desastres naturales o intencionales	Vulnerabilidad	Daños y Perdida de la Información
Incendios -- Cableado estructurado	Desastres naturales o intencionales	Vulnerabilidad	Daños y Perdida de la Información
Incendios -- UPS	Desastres naturales o intencionales	Vulnerabilidad	Daños y Perdida de la Información
Incendios -- Impresoras y Scaner	Desastres naturales o intencionales	Vulnerabilidad	Daños y Perdida de la Información
Incendios -- Sistema de camaras vigilancia	Desastres naturales o intencionales	Vulnerabilidad	Daños y Perdida de la Información
Incendios -- Servidores correo,archivos, web	Desastres naturales o intencionales	Vulnerabilidad	Daños y Perdida de la Información
Incendios -- Controlador de dominio Directorio Activo	Desastres naturales o intencionales	Vulnerabilidad	Daños y Perdida de la Información
Terremotos -- Routes	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Terremotos -- Swiches	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Terremotos -- Estaciones de trabajo	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Terremotos -- Acces Point	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Terremotos -- Dispositivos moviles y electronicos	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Terremotos -- Control de acceso ingreso	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Terremotos -- Cableado estructurado	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Terremotos -- UPS	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Terremotos -- Impresoras y Scaner	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Terremotos -- Sistema de camaras vigilancia	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Terremotos -- Servidores correo,archivos, web	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Terremotos -- Sistemas de Informacion	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Terremotos -- Controlador de dominio Directorio Activo	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Tormentas eléctricas -- Routes	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Tormentas eléctricas -- Swiches	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Tormentas eléctricas -- Estaciones de trabajo	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Tormentas eléctricas -- Acces Point	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Tormentas eléctricas -- Dispositivos moviles y electronicos	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Tormentas eléctricas -- Cableado estructurado	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Tormentas eléctricas -- UPS	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Tormentas eléctricas -- Impresoras y Scaner	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Tormentas eléctricas -- Sistema de camaras vigilancia	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Tormentas eléctricas -- Servidores correo,archivos, web	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Tormentas eléctricas -- Sistemas de Informacion	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Tormentas eléctricas -- Controlador de dominio Directorio Activo	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Inundaciones -- Routes	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Inundaciones -- Swiches	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Inundaciones -- Estaciones de trabajo	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Inundaciones -- Acces Point	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Inundaciones -- Dispositivos moviles y electronicos	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Inundaciones -- Control de acceso ingreso	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Inundaciones -- Cableado estructurado	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Inundaciones -- UPS	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Inundaciones -- Impresoras y Scaner	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Inundaciones -- Servidores correo,archivos, web	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Inundaciones -- Sistemas de Informacion	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Inundaciones -- Controlador de dominio Directorio Activo	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Alud -- Routes	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Alud -- Swiches	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Alud -- Estaciones de trabajo	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Alud -- Acces Point	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Alud -- Dispositivos moviles y electronicos	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Alud -- Control de acceso ingreso	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Alud -- Cableado estructurado	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Alud -- UPS	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Alud -- Impresoras y Scaner	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Alud -- Sistema de camaras vigilancia	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Alud -- Servidores correo,archivos, web	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Alud -- Sistemas de Informacion	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Alud -- Controlador de dominio Directorio Activo	Desastres naturales	Vulnerabilidad	Daños y Perdida de la Información
Atentados terroristas -- Routes	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Atentados terroristas -- Swiches	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Atentados terroristas -- Estaciones de trabajo	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Atentados terroristas -- Acces Point	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Atentados terroristas -- Dispositivos moviles y electronicos	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Atentados terroristas -- Control de acceso ingreso	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Atentados terroristas -- Cableado estructurado	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Atentados terroristas -- UPS	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Atentados terroristas -- Impresoras y Scaner	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Atentados terroristas -- Sistema de camaras vigilancia	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Atentados terroristas -- Servidores correo,archivos, web	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Atentados terroristas -- Bases de Datos	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Atentados terroristas -- Sistemas de Informacion	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Atentados terroristas -- Controlador de dominio Directorio Activo	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Manifestaciones -- Routes	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Manifestaciones -- Swiches	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Manifestaciones -- Estaciones de trabajo	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Manifestaciones -- Acces Point	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Manifestaciones -- Dispositivos moviles y electronicos	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Manifestaciones -- Control de acceso ingreso	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Manifestaciones -- Cableado estructurado	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Manifestaciones -- UPS	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Manifestaciones -- Impresoras y Scaner	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Manifestaciones -- Sistema de camaras vigilancia	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Manifestaciones -- Servidores correo,archivos, web	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Manifestaciones -- Sistemas de Informacion	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Manifestaciones -- Controlador de dominio Directorio Activo	Ataque	Vulnerabilidad	Daños y Perdida de la Información
Orden Público -- Estaciones de trabajo	Ataque o delincuencia	Vulnerabilidad	Daños y Perdida de la Información
Orden Público -- Acces Point	Ataque o delincuencia	Vulnerabilidad	Daños y Perdida de la Información
Orden Público -- Dispositivos moviles y electronicos	Ataque o delincuencia	Vulnerabilidad	Daños y Perdida de la Información
Orden Público -- Control de acceso ingreso	Ataque o delincuencia	Vulnerabilidad	Daños y Perdida de la Información
Orden Público -- Cableado estructurado	Ataque o delincuencia	Vulnerabilidad	Daños y Perdida de la Información
Orden Público -- UPS	Ataque o delincuencia	Vulnerabilidad	Daños y Perdida de la Información
Orden Público -- Impresoras y Scaner	Ataque o delincuencia	Vulnerabilidad	Daños y Perdida de la Información
Orden Público -- Sistema de camaras vigilancia	Ataque o delincuencia	Vulnerabilidad	Daños y Perdida de la Información

Calificación con Controles

ESCENARIO	PROBABILIDAD		IMPACTO OPERACIÓN		Riesgo P*Impacto	IMPACTO INFORMACIÓN		IMPACTO IMAGEN	
Suplantacion de identidad -- Estaciones de trabajo	Posible	3	Insignificante	1	3	Insignificante	1	Medio	3
Suplantacion de identidad -- Servidores Virtuales	Posible	3	Medio	3	9	Menor	2	Mayor	4
Suplantacion de identidad -- Servidores correo,archivos, web	Posible	3	Medio	3	9	Mayor	4	Mayor	4
Suplantacion de identidad -- Informacion	Posible	3	Insignificante	1	3	Menor	2	Mayor	4
Virus-malware -- Routes	Ocasional	2	Menor	2	4	Menor	2	Medio	3
Virus-malware -- Swiches	Ocasional	2	Mayor	4	8	Menor	2	Medio	3
Virus-malware -- Estaciones de trabajo	Posible	3	Insignificante	1	3	Insignificante	1	Medio	3
Virus-malware -- Acces Point	Posible	3	Menor	2	6	Insignificante	1	Medio	3
Virus-malware -- Dispositivos moviles y electronicos	Ocasional	2	Menor	2	4	Insignificante	1	Medio	3
Virus-malware -- Cableado estructurado	Posible	3	Mayor	4	12	Insignificante	1	Menor	2
Virus-malware -- Impresoras y Scaner	Ocasional	2	Menor	2	4	Menor	2	Menor	2
Virus-malware -- Sistema de camaras vigilancia	Ocasional	2	Mayor	4	8	Menor	2	Medio	3
Virus-malware -- Servidores Virtuales	Posible	3	Menor	2	3	Menor	2	Mayor	4
Virus-malware -- Servidores correo,archivos, web	Posible	3	Menor	2	3	Mayor	4	Mayor	4
Virus-malware -- Bases de Datos	Posible	3	Menor	2	6	Mayor	4	Mayor	4
Virus-malware -- Sistemas de Informacion	Ocasional	2	Menor	2	4	Mayor	4	Mayor	4
Virus-malware -- Controlador de dominio Directorio Activo	Ocasional	2	Menor	2	4	Menor	2	Medio	3
Virus-malware -- Licencias	Muy ocasional	1	Insignificante	1	1	Medio	3	Medio	3
Robo de información o (Ransomware) -- Estaciones de trabajo	Casi seguro	4	Insignificante	1	4	Insignificante	1	Menor	2
Robo de información o (Ransomware) -- Dispositivos moviles y electronicos	Posible	3	Menor	2	6	Menor	2	Menor	2
Robo de información o (Ransomware) -- Cableado estructurado	Ocasional	2	Menor	2	4	Insignificante	1	Menor	2
Robo de información o (Ransomware) -- Sistema de camaras vigilancia	Muy ocasional	1	Insignificante	1	1	Medio	3	Medio	3
Robo de información o (Ransomware) -- Servidores Virtuales	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Robo de información o (Ransomware) -- Servidores correo,archivos, web	Muy ocasional	1	Menor	2	2	Mayor	4	Medio	3
Robo de información o (Ransomware) -- Bases de Datos	Ocasional	2	Menor	2	4	Mayor	4	Mayor	4
Robo de información o (Ransomware) -- Sistemas de Informacion	Posible	3	Menor	2	6	Superior	5	Mayor	4
Robo de información o (Ransomware) -- Informacion	Posible	3	Insignificante	1	3	Superior	5	Medio	3
Robo de información o (Ransomware) -- Licencias	Ocasional	2	Medio	3	6	Medio	3	Menor	2
Robo de infraestructura -- Routes	Muy ocasional	1	Menor	2	2	Insignificante	1	Mayor	4
Robo de infraestructura -- Swiches	Muy ocasional	1	Mayor	4	4	Mayor	4	Mayor	4
Robo de infraestructura -- Estaciones de trabajo	Ocasional	2	Insignificante	1	2	Insignificante	1	Mayor	4
Robo de infraestructura -- Acces Point	Muy ocasional	1	Mayor	4	4	Insignificante	1	Mayor	4
Robo de infraestructura -- Dispositivos moviles y electronicos	Muy ocasional	1	Insignificante	1	1	Mayor	4	Mayor	4
Robo de infraestructura -- Control de acceso ingreso	Muy ocasional	1	Mayor	4	4	Medio	3	Mayor	4
Robo de infraestructura -- Cableado estructurado	Muy ocasional	1	Mayor	4	4	Medio	3	Medio	3
Robo de infraestructura -- Impresoras y Scaner	Muy ocasional	1	Mayor	4	4	Menor	2	Medio	3
Robo de infraestructura -- Sistema de camaras vigilancia	Muy ocasional	1	Mayor	4	4	Medio	3	Medio	3
Robo de infraestructura -- Controlador de dominio Directorio Activo	Muy ocasional	1	Mayor	4	4	Menor	2	Medio	3
SQL Injection (bases de datos) -- Servidores Virtuales	Ocasional	2	Mayor	4	8	Superior	5	Mayor	4
SQL Injection (bases de datos) -- Servidores correo,archivos, web	Ocasional	2	Mayor	4	8	Superior	5	Mayor	4
SQL Injection (bases de datos) -- Bases de Datos	Ocasional	2	Mayor	4	8	Superior	5	Mayor	4
SQL Injection (bases de datos) -- Informacion	Ocasional	2	Mayor	4	8	Superior	5	Mayor	4
Alteración maliciosa de la información -- Estaciones de trabajo	Ocasional	2	Insignificante	1	2	Menor	2	Medio	3
Alteración maliciosa de la información -- Impresoras y Scaner	Ocasional	2	Menor	2	4	Insignificante	1	Medio	3
Alteración maliciosa de la información -- Sistema de camaras vigilancia	Posible	3	Medio	3	9	Menor	2	Medio	3
Alteración maliciosa de la información -- Servidores Virtuales	Posible	3	Medio	3	9	Menor	2	Medio	3
Alteración maliciosa de la información -- Servidores correo,archivos, web	Posible	3	Medio	3	9	Mayor	4	Medio	3
Alteración maliciosa de la información -- Sistemas de Informacion	Posible	3	Menor	2	6	Mayor	4	Medio	3
Alteración maliciosa de la información -- Controlador de dominio Directorio Acti	Ocasional	2	Insignificante	1	2	Menor	2	Medio	3
Alteración maliciosa de la información -- Informacion	Posible	3	Insignificante	1	3	Superior	5	Medio	3
Alteración maliciosa de la información -- Licencias	Ocasional	2	Medio	3	6	Medio	3	Medio	3
Sniffers (trafico de datos) -- Routes	Ocasional	2	Menor	2	4	Menor	2	Medio	3
Sniffers (trafico de datos) -- Swiches	Ocasional	2	Mayor	4	8	Menor	2	Medio	3
Sniffers (trafico de datos) -- Acces Point	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Sniffers (trafico de datos) -- Cableado estructurado	Posible	3	Mayor	4	12	Menor	2	Medio	3
Sniffers (trafico de datos) -- Sistema de camaras vigilancia	Posible	3	Menor	2	6	Medio	3	Medio	3
Sniffers (trafico de datos) -- Servidores Virtuales	Muy ocasional	1	Mayor	4	4	Mayor	4	Medio	3
Denegacion de servicios -- Swiches	Muy ocasional	1	Menor	2	2	Mayor	4	Medio	3
Denegacion de servicios -- Estaciones de trabajo	Ocasional	2	Menor	2	4	Mayor	4	Medio	3
Denegacion de servicios -- Sistema de camaras vigilancia	Posible	3	Menor	2	6	Medio	3	Medio	3
Denegacion de servicios -- Servidores Virtuales	Posible	3	Menor	2	6	Superior	5	Mayor	4
Denegacion de servicios -- Servidores correo,archivos, web	Ocasional	2	Menor	2	4	Superior	5	Mayor	4
Denegacion de servicios -- Bases de Datos	Posible	3	Menor	2	6	Superior	5	Mayor	4
Denegacion de servicios -- Sistemas de Informacion	Posible	3	Medio	3	9	Superior	5	Mayor	4
Denegacion de servicios -- Controlador de dominio Directorio Activo	Muy ocasional	1	Menor	2	2	Superior	5	Medio	3
Denegacion de servicios -- Informacion	Posible	3	Menor	2	6	Superior	5	Mayor	4
Conexiones o accesos no autorizadas -- Routes	Posible	3	Menor	2	6	Mayor	4	Medio	3
Conexiones o accesos no autorizadas -- Swiches	Posible	3	Menor	2	6	Mayor	4	Medio	3
Conexiones o accesos no autorizadas -- Estaciones de trabajo	Posible	3	Insignificante	1	3	Insignificante	1	Medio	3
Conexiones o accesos no autorizadas -- Acces Point	Posible	3	Menor	2	6	Menor	2	Medio	3
Conexiones o accesos no autorizadas -- Cableado estructurado	Posible	3	Menor	2	6	Mayor	4	Medio	3
Conexiones o accesos no autorizadas -- Impresoras y Scaner	Ocasional	2	Insignificante	1	2	Insignificante	1	Medio	3
Conexiones o accesos no autorizadas -- Sistema de camaras vigilancia	Posible	3	Menor	2	6	Medio	3	Medio	3
Conexiones o accesos no autorizadas -- Servidores Virtuales	Ocasional	2	Menor	2	4	Mayor	4	Mayor	4
Conexiones o accesos no autorizadas -- Servidores correo,archivos, web	Ocasional	2	Menor	2	4	Superior	5	Mayor	4
Conexiones o accesos no autorizadas -- Bases de Datos	Posible	3	Menor	2	6	Superior	5	Medio	3
Conexiones o accesos no autorizadas -- Sistemas de Informacion	Posible	3	Medio	3	9	Superior	5	Mayor	4
Conexiones o accesos no autorizadas -- Informacion	Posible	3	Mayor	4	12	Superior	5	Mayor	4
Spammer -- Estaciones de trabajo	Ocasional	2	Insignificante	1	2	Mayor	4	Menor	2
Spammer -- Servidores correo,archivos, web	Ocasional	2	Menor	2	4	Superior	5	Medio	3
Spammer -- Informacion	Ocasional	2	Menor	2	4	Superior	5	Medio	3
Ingenieria social -- Estaciones de trabajo	Casi seguro	4	Insignificante	1	4	Menor	2	Menor	2
Ingenieria social -- Dispositivos moviles y electronicos	Posible	3	Insignificante	1	3	Menor	2	Menor	2
Ingenieria social -- Cableado estructurado	Posible	3	Menor	2	6	Menor	2	Medio	3
Ingenieria social -- Impresoras y Scaner	Posible	3	Insignificante	1	3	Menor	2	Menor	2
Ingenieria social -- Sistema de camaras vigilancia	Posible	3	Menor	2	6	Medio	3	Medio	3
Ingenieria social -- Servidores Virtuales	Ocasional	2	Menor	2	4	Mayor	4	Medio	3
Ingenieria social -- Bases de Datos	Ocasional	2	Menor	2	4	Superior	5	Medio	3
Ingenieria social -- Sistemas de Informacion	Posible	3	Menor	2	6	Superior	5	Medio	3
Ingenieria social -- Controlador de dominio Directorio Activo	Ocasional	2	Menor	2	4	Mayor	4	Medio	3
Ingenieria social -- Informacion	Ocasional	2	Insignificante	1	2	Superior	5	Menor	2
Ingenieria social -- Licencias	Ocasional	2	Medio	3	6	Medio	3	Menor	2
ex-empleados o empleados insatisfechos -- Estaciones de trabajo	Posible	3	Menor	2	6	Insignificante	1	Menor	2
ex-empleados o empleados insatisfechos -- Dispositivos moviles y electronico	Posible	3	Menor	2	6	Insignificante	1	Menor	2
ex-empleados o empleados insatisfechos -- Control de acceso ingreso	Posible	3	Menor	2	6	Menor	2	Menor	2

	Calificación con Controles								
ESCENARIO	PROBABILIDAD		IMPACTO OPERACIÓN		Riesgo P*Impacto	IMPACTO INFORMACIÓN		IMPACTO IMAGEN	
ex-empleados o empleados insatisfechos -- Cableado estructurado	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
ex-empleados o empleados insatisfechos -- UPS	Muy ocasional	1	Medio	3	3	Insignificante	1	Medio	3
ex-empleados o empleados insatisfechos -- Impresoras y Scaner	Posible	3	Insignificante	1	3	Insignificante	1	Menor	2
ex-empleados o empleados insatisfechos -- Sistema de camaras vigilancia	Muy ocasional	1	Menor	2	2	Medio	3	Medio	3
ex-empleados o empleados insatisfechos -- Sistemas de Informacion	Muy ocasional	1	Menor	2	2	Medio	3	Medio	3
ex-empleados o empleados insatisfechos -- Controlador de dominio Directorio	Ocasional	2	Menor	2	4	Menor	2	Medio	3
ex-empleados o empleados insatisfechos -- Informacion	Posible	3	Menor	2	6	Superior	5	Medio	3
Incendios -- Routes	Muy ocasional	1	Mayor	4	4	Menor	2	Medio	3
Incendios -- Swiches	Muy ocasional	1	Mayor	4	4	Menor	2	Mayor	4
Incendios -- Estaciones de trabajo	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Medio	3
Incendios -- Acces Point	Muy ocasional	1	Mayor	4	4	Insignificante	1	Medio	3
Incendios -- Dispositivos moviles y electronicos	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Medio	3
Incendios -- Control de acceso ingreso	Muy ocasional	1	Medio	3	3	Medio	3	Medio	3
Incendios -- Cableado estructurado	Muy ocasional	1	Medio	3	3	Medio	3	Medio	3
Incendios -- UPS	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Medio	3
Incendios -- Impresoras y Scaner	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Medio	3
Incendios -- Sistema de camaras vigilancia	Muy ocasional	1	Medio	3	3	Medio	3	Medio	3
Incendios -- Servidores correo,archivos, web	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Terremotos -- Swiches	Muy ocasional	1	Mayor	4	4	Menor	2	Medio	3
Terremotos -- Estaciones de trabajo	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Medio	3
Terremotos -- Acces Point	Muy ocasional	1	Menor	2	2	Insignificante	1	Medio	3
Terremotos -- Dispositivos moviles y electronicos	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Menor	2
Terremotos -- Control de acceso ingreso	Muy ocasional	1	Medio	3	3	Medio	3	Menor	2
Terremotos -- Cableado estructurado	Muy ocasional	1	Mayor	4	4	Medio	3	Medio	3
Terremotos -- UPS	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Medio	3
Terremotos -- Sistema de camaras vigilancia	Muy ocasional	1	Medio	3	3	Medio	3	Menor	2
Terremotos -- Servidores correo,archivos, web	Muy ocasional	1	Menor	2	2	Menor	2	Menor	2
Terremotos -- Sistemas de Informacion	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Terremotos -- Controlador de dominio Directorio Activo	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Tormentas eléctricas -- Routes	Muy ocasional	1	Mayor	4	4	Menor	2	Medio	3
Tormentas eléctricas -- Estaciones de trabajo	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Menor	2
Tormentas eléctricas -- Acces Point	Muy ocasional	1	Menor	2	2	Insignificante	1	Menor	2
Tormentas eléctricas -- Dispositivos moviles y electronicos	Muy ocasional	1	Mayor	4	4	Insignificante	1	Menor	2
Tormentas eléctricas -- Cableado estructurado	Muy ocasional	1	Mayor	4	4	Menor	2	Medio	3
Tormentas eléctricas -- Sistema de camaras vigilancia	Muy ocasional	1	Medio	3	3	Medio	3	Medio	3
Tormentas eléctricas -- Servidores correo,archivos, web	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Tormentas eléctricas -- Sistemas de Informacion	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Tormentas eléctricas -- Controlador de dominio Directorio Activo	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Inundaciones -- Routes	Muy ocasional	1	Mayor	4	4	Menor	2	Medio	3
Inundaciones -- Swiches	Muy ocasional	1	Mayor	4	4	Menor	2	Medio	3
Inundaciones -- Estaciones de trabajo	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Menor	2
Inundaciones -- Acces Point	Muy ocasional	1	Menor	2	2	Insignificante	1	Menor	2
Inundaciones -- Dispositivos moviles y electronicos	Muy ocasional	1	Mayor	4	4	Menor	2	Menor	2
Inundaciones -- Cableado estructurado	Muy ocasional	1	Mayor	4	4	Medio	3	Medio	3
Inundaciones -- Impresoras y Scaner	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Menor	2
Inundaciones -- Servidores correo,archivos, web	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Inundaciones -- Sistemas de Informacion	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Inundaciones -- Controlador de dominio Directorio Activo	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Alud -- Routes	Muy ocasional	1	Mayor	4	4	Menor	2	Medio	3
Alud -- Swiches	Muy ocasional	1	Mayor	4	4	Menor	2	Medio	3
Alud -- Estaciones de trabajo	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Menor	2
Alud -- Acces Point	Muy ocasional	1	Menor	2	2	Insignificante	1	Menor	2
Alud -- Dispositivos moviles y electronicos	Muy ocasional	1	Mayor	4	4	Menor	2	Menor	2
Alud -- UPS	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Menor	2
Atentados terroristas -- UPS	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Menor	2
Atentados terroristas -- Impresoras y Scaner	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Menor	2
Atentados terroristas -- Sistema de camaras vigilancia	Muy ocasional	1	Mayor	4	4	Medio	3	Medio	3
Atentados terroristas -- Servidores correo,archivos, web	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Atentados terroristas -- Bases de Datos	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Atentados terroristas -- Sistemas de Informacion	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Atentados terroristas -- Controlador de dominio Directorio Activo	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Manifestaciones -- Routes	Muy ocasional	1	Mayor	4	4	Menor	2	Menor	2
Manifestaciones -- Estaciones de trabajo	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Menor	2
Manifestaciones -- Acces Point	Muy ocasional	1	Menor	2	2	Insignificante	1	Menor	2
Manifestaciones -- Dispositivos moviles y electronicos	Muy ocasional	1	Mayor	4	4	Menor	2	Menor	2
Manifestaciones -- Control de acceso ingreso	Muy ocasional	1	Mayor	4	4	Menor	2	Menor	2
Manifestaciones -- Cableado estructurado	Muy ocasional	1	Mayor	4	4	Menor	2	Medio	3
Manifestaciones -- UPS	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Menor	2
Manifestaciones -- Impresoras y Scaner	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Menor	2
Manifestaciones -- Sistema de camaras vigilancia	Muy ocasional	1	Medio	3	3	Medio	3	Menor	2
Manifestaciones -- Servidores correo,archivos, web	Muy ocasional	1	Menor	2	2	Menor	2	Medio	3
Manifestaciones -- Sistemas de Informacion	Muy ocasional	1	Menor	2	2	Menor	2	Menor	2
Manifestaciones -- Controlador de dominio Directorio Activo	Muy ocasional	1	Menor	2	2	Menor	2	Menor	2
Orden Público -- Estaciones de trabajo	Ocasional	2	Insignificante	1	2	Insignificante	1	Menor	2
Orden Público -- Acces Point	Ocasional	2	Menor	2	4	Insignificante	1	Menor	2
Orden Público -- Dispositivos moviles y electronicos	Ocasional	2	Mayor	4	8	Menor	2	Menor	2
Orden Público -- Control de acceso ingreso	Posible	3	Mayor	4	12	Menor	2	Menor	2
Orden Público -- Cableado estructurado	Muy ocasional	1	Mayor	4	4	Menor	2	Medio	3
Orden Público -- UPS	Muy ocasional	1	Insignificante	1	1	Insignificante	1	Menor	2
Orden Público -- Impresoras y Scaner	Ocasional	2	Insignificante	1	2	Insignificante	1	Menor	2
Orden Público -- Sistema de camaras vigilancia	Ocasional	2	Medio	3	6	Medio	3	Menor	2

Las siguientes tablas nos muestra un resumen del análisis de riesgo realizado y cuáles de estos riesgos serán tratados en el plan de cultura.

ACEPTABILIDAD CON CONTROLES (operación)

DISTRIBUCIÒN PORCENTUAL		
ZONA	%	Total riesgos
Bajo	50,568182	89
Medio	22,159091	39
Medio-Alto	25	44
Altos	2,2727273	4

ACEPTABILIDAD CON CONTROLES (Información)

DISTRIBUCIÒN PORCENTUAL		
ZONA	%	Total riesgos
Bajo	52,840909	93
Medio	19,886364	35
Medio-Alto	10,227273	18
Altos	17,045455	30

ACEPTABILIDAD CON CONTROLES (Imagen)

DISTRIBUCIÒN PORCENTUAL		
ZONA	%	Total riesgos
Bajo	24,840764	39
Medio	52,866242	83
Medio-Alto	14,012739	22
Altos	8,2802548	13

Todas estas estrategias se apoyan en la movilidad y la creación de nuevos servicios de TI, los cuales tienen vulnerabilidades, amenazas y riesgos que son mitigados con la implementación de nuevos controles, la mejora de los ya existentes o la transferencia de éstos a terceras partes. Para que estos controles sean efectivos, el conocimiento y la sensibilización a los empleados, contratistas y terceros son fundamentales.

RIESGOS ALTOS

- **Ataques de malware**: Servidores web, correo, archivos/Bases de Datos/Dispositivos móviles/Estaciones de trabajo.
- **Phishing y Pharming**: Servidor web, correo, archivos.
- **Robo de información**: Servidores web, correo, archivos / Servidor Base de/datos/ Estaciones de Trabajo
- **Robo de claves de autenticación:** Servidor Controlador de dominio/ Servidores de correo, archivos, web/Servidor Bases de Datos/ Estaciones de trabajo/ Dispositivos móviles.

RIESGOS MODERADOS

- **Instalación de software ilegal:** Estaciones de trabajo/ Dispositivos Móviles.
- Desconfiguración: Servidor Controlador de Dominio/ Servidor Correo, web, Archivo/Base de Datos/ Dispositivos Móviles/ Controlador de Dominio.
- **Fallas en la Comunicación:** Servidor de Correo, web, archivo.

VALORACIÓN DEL RIESGO

RIESGOS ALTOS (Considerando los controles actuales)	TRATAMIENTO				DESCRIPCION DEL CONTROL	RESPONSABLE	CONTROL IMPLEMENTADO/RESULTADO	CONTROL ANEXO A.
	Aceptarlo	Evitarlo	Controlarlo	Transferirlo				
Virus-malware -- Servidores de correo, web, archivos			X		* Tener instalado Antivirus licenciado y actualizado. * Controlar política a nivel de software que controle la gestión sobre los puertos USB en las estaciones de trabajo y servidores Windows	Analista de seguridad	* Controlar propagación virus. * Antivirus actualizado	A.5, A.6.2, A.12.2, A.12.3., A.13,
Scanner Puertos abiertos -- controlador de dominio			X		Cerrar puertos que no son utilizados y monitoreo de los que están abiertos, habilitar auditoria.	Analista de seguridad	* No ser hackeados. * Cerrado de puertos que no se requieren.	A.9, A.13
SQL injection -- Bases de Datos			X		Código seguro en la aplicación web.	Analista de Infraestructura	* No acceder a las Bases de datos, personal no autorizado. * controlar perfiles y roles de acceso	A.6, A.9.3, A.14
Robo de información -- Bases de Datos			X		Política control de acceso al servidor base de datos.	Analista de Infraestructura	* Control de acceso. * Realizar copias de seguridad	A.5, A.7, A.8, A.9, A.11., A.12.3
Spammer -- Servidores de correo, web, archivos.			X		Tener instalado antivirus licenciado, tener un firewall para administración de puertos, aplicaciones, protección de intrusos y tráfico de internet entre otras.	Analista de seguridad	* Minimizar riesgo de denegación de servicio y congestión en la red. * Implementación de actualizaciones	A.12.2, A.13,

Robo -- Información			X		*Política control de acceso, política de seguridad de la información y socialización Campañas de sensibilización a los usuarios finales. *Capacitación al personal en seguridad de la información.	Analista de seguridad, usuarios	* Control de acceso, sensibilización de los usuarios. * Realizar copias de seguridad	A.5, A.6.2, A.7, A.8, A.9, A.11, A.12.3, A.13
Robo de información -- controlador de dominio			X		Política control de acceso. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.	Analista de Infraestructura	* Control de acceso ingreso a los recursos. * Realizar copias de seguridad	A.5, A.6, A.7, A.8, A.9, A.9.2, A.11, A.12.3,
Alteración maliciosa de la información -- Bases de Datos			X		Política control de acceso, monitoreo de logueo.	Analista de Infraestructura	* Control de acceso	A.5, A.7, A.8, A.9, A.11, A.12.2, A.12.3, A.12.4., A.13, A
suplantación de identidad -- Servidores Virtuales			X		Política control de acceso, monitoreo de contraseñas.	Analista de seguridad	* Minimizar riesgos de acceso al servicio	A.5, A.9,

Escenario de riesgo (Activo-Amenaza)	PROBABILIDAD					IMPACTO
	Habilidad	Motivación	Recursos	Accesabilidad	TOTAL	
Virus-malware -- Servidores de correo,web, archivo	3	2	3	2	Alto-3	3
Scaner Puertos abiertos -- controlador de dominio	3	3	3	2	Alto-3	3
SQL injection -- Bases de Datos	2	3	3	3	Alto-3	3
Robo de información -- Bases de Datos	3	3	3	3	Alto-3	3
Spammer -- Servidores de correo,web,archivos.	3	1	1	1	Medio-2	2
Robo -- Información	3	1	3	3	Alto-3	3
Robo de información -- controlador de dominio	3	3	3	3	Alto-3	3
Alteración maliciosa de la información -- Bases de Datos	3	1	3	3	Alto-3	3
suplantacion de identidad -- Servidores Virtuales	3	2	3	3	Alto-3	3

PROBABILIDAD		
Valor	Habilidad	Nivel de conocimiento y experiencia requerido para explotar una vulnerabilidad.
1	Alto	Se requiere altos conocimientos sobre el sistema o plataforma, con temas especializados de SO y redes.
2	Medio	Se requieren conocimientos básicos para realizar tareas administrativas.
3	Bajo	Se requiere de conocimientos elementales de operación y administración de computadores, redes, de sentencias SQL o comandos basicos a nivel de S.O.

IMPACTO: Confidencialidad, Integridad y Disponibilidad		
1	Bajo	Efecto adverso en un grado y duración tales que sólo tienen incidencia en lo procesos internos sin consecuencias trascendentes a nivel general de la entidad y sin representar pérdidas significativas
2	Medio	Efecto adverso en un grado y duración tales que sólo tienen incidencia en los procesos internos, sin llegar a tener consecuencias trascendentes a nivel corporativo, aunque con pérdidas significativas, financieras o de otra índole.
3	Alto	Efecto adverso severo en un grado y duración tales que afectan las funciones primarias de la entidad, comprometiendo su capacidad competitiva

PLAN CULTURAL

El plan de cultura se basa en el análisis de riesgo de los activos de información, de los cuales los riesgos catalogados como altos y moderados serán el foco de sensibilización.

PLAN CULTURAL			
Objetivo: Crear un plan de cultura y socialización para los empleados y usuarios en la seguridad y el acceso a la información.			
Medios	**Mensajes**	**Canal Principal**	**Frecuencia**
Intranet	* El buen uso de la contraseña * Como salvaguardar la información * Cambios y desiciones	* Mensajes del jefe * Mensajes del encargado de la seguridad informatica * Correos masivos	* Quincenal * Cuando se haga algun cambio en las politicas
Tips de seguridad	* Resolucion Politicas de Seguridad de la Información. * Recomendaciones y acuerdos de confidencialidad. * Realizar depuraciones y eliminar informacion que ya no es útil.	* Personal de sistemas * Mensajes en la pagina web (Intranet) para los usuarios * Correos masivos	*Mensual
Usuarios finales (charla seguridad de la Información)	*Concientizar al personal de los riesgos en el manejo de contraseñas. * Informar de la vulnerabilidad de la información ante ataques * Noticias Falsas, Secuestro del WhatsApp ,Suplantación de Identidad,secuestro de la informacion. * Malas Prácticas de Seguridad de la Información	* Mensajes del jefe * Reuniones con el area de seguridad de la información. * charla de sensibilización * Mensajes en carteleras	* Periodicamente según la necesidad * Mensual
Mensajes para las sedes	* información de los cambios y desiciones del área de sistemas. * Avances en implementaciones tecnológicas	*Personal Interno de cada sede	*Quincenal

Alcance del plan de cultura de seguridad de información

El plan de cultura tiene como alcance el planear, diseñar y ejecutar las capacitaciones, charlas, conferencias, boletines y correos de sensibilización para que los empleados, terceros y personal directivo conozcan las amenazas, los riesgos y los controles que se tienen y que son catalogados con un riesgo residual alto o moderado.

Áreas de apoyo

El área de seguridad de T.I. es la responsable de coordinar los programas de capacitación, sensibilización y entrenamiento en seguridad de la información y el área que participa en el proceso de gestión de cultura de seguridad es: Talento humano.

Diseño de contenidos y sus medios de difusión

La esencia de la seguridad de información es la “Cultura de seguridad”, y para ello se debe crear conciencia sobre actos o actuaciones inseguras, reduciendo las condiciones de inseguridad y la importancia de protección de los activos de información.

Medios utilizados para generar plan de cultura de seguridad de la información

 **Medios**	 **Mensajes Claves**	 **Canales Principales**	 **Frecuencia**	 **Retroalimentación**
Plan de Cultura dirigido a los Directivos para mitigar los riesgos de: Fuga de la información, desconfiguración de equipos y fallas en la comunicación				
Presentación	***)** Exponer las fallas de seguridad que se tienen , causas y consecuencias y la pérdida a la que se esta sometida si no se atacan las vulnerabilidades. *) Crear conciencia en los directivos sobre los riesgos a los que se esta expuesto a diario. Dar a conocer casos reales.	*) Reunión con la Gerencia y directivos	*) anual	Mostrar con indicadores, los resultados del analisis de vulnerabilidades.
Plan de cultura dirigido a los analistas de infraestructura y desarrolladores				
Capacitaciones	***)** Actualización en temas de infraestructura y telecomunicaciones. *) Minimizar el riesgo de gestionar mal la seguridad en las redes. *) Actualización en el manejo de la seguridad en	*) Seminarios sobre temas de seguridad.	*) Semestral	*) Indicadores de incidentes

	las aplicaciones (en caso de desarrollo de software).			
Plan de Cultura dirigido a los empleados, entrenadores, deportistas, contratistas y terceros para mitigar los riesgos de: Ataques de malware, Phishing y Pharming, ransomware, instalación de software ilegal en las estaciones de trabajo y equipos móviles poder así evitar el daño a los equipos y la fuga o robo de información.				
Conferencias sensibilización	*) Se necesita socializar a los empleados, entrenadores, deportistas, contratistas y terceros con la resolución de la Política de Seguridad de la información en general. *) Sensibilizar y crear conciencia a los empleados, entrenadores, deportistas, contratistas sobre la Seguridad de la información.	Citación por parte de sistemas y el área de Talento Humano en diferentes horarios y por grupos	*) Anual	Evaluación al terminar la conferencia. Listado de asistencia
Carteles físicos en sitio	publicación de información, letreros o lemas alusivos a la seguridad de la información en cada una de las carteleras del Instituto.	El personal de Talento Humano y comunicaciones	1 publicación mensual- depende de los tips de seguridad de la información	Evaluar al personal en función de los carteles, Formulario a través de la Intranet o correo electrónico.
Campañas y tips por correos electrónicos	*) Recordar y poner en práctica los Tips informáticos de seguridad de la información que se puedan aplicar en la oficina y en casa. *) El contenido es información muy concisa sobre la Resolución 514 de 2020 las políticas, estándares de seguridad y uso de recursos informáticos en la entidad y otros temas de actualidad sobre seguridad.	Envió de correos electrónicos por el área de Comunicaciones y sistemas. Y la intranet	2 veces al mes	Retroalimentación en la charla de seguridad de la información, se evalúa.

Capacitación por áreas	*Es reforzar el conocimiento de seguridad en las áreas que se detecte falencias o incidentes recurrentes en algún tema de seguridad. Se determina a través del indicador de la mesa de servicios. *) Capacitación presencial a áreas específicas del Instituto.	Citación por correo electrónico del área de talento humano o sistemas.	1 vez al año	Retroalimentación al finalizar la charla
Pruebas de hacking ético	Colocar o enviar señuelos en archivos que disparen macros inofensivas.	Lo realiza el analista de seguridad o contratar un tercero para realizar dicha prueba	1 vez al mes	En cada prueba se envía indicador de las personas que fueron evaluadas y su respectivo informe.
Campaña demuéstranos que sabes de seguridad	*) Medir el nivel de conocimiento del personal sobre Seguridad de la información.	El área de comunicaciones promoviendo la campaña y el área de talento humano con el detalle.	2 veces al año	Al final del semestre enviar un correo con una actividad y un concurso entregar un regalo (memorias USB, un bono, disco duro extraíble, etc..)
Resolución Políticas de seguridad de la información	Entrega física de la Resolución de la política de seguridad de información en el momento de la Inducción al ingreso A INDEPORTES ANTIOQUIA.	Área Talento humano	1 vez al año	Es socializada por el área de Talento humano, en la charla de Inducción.

- Ejemplo de correos de sensibilización:

Temas De Boletines Mensuales 2022:

Mes	Tema mensual	Descripción
Diciembre	Seguridad en tu PC y dispositivos móviles	Nos da pauta como asegurar las estaciones de trabajo, temas como cifrado de portátiles, instalación de antivirus, actualizaciones y conexión a redes inalámbricas no seguras. Dar a conocer tips de seguridad para minimizar el riesgo de fuga de información en un dispositivo móvil.
Enero	Seguridad en la nube	Resolver inquietudes como que es la nube, que debo tener en cuenta con los datos que subo en la nube, conexión a servicio de la nube de forma segura.
Febrero	Mantener las actualizaciones del software	Boletín que da a conocer que es la actualización del sistema operativo, que debemos tener en cuenta cuando se instala un programa, tipos de licencias, proceso de instalación de programas free.
Marzo	Seguridad en redes sociales y mensajería gratuita.	Dar a conocer los riesgos al momento de utilizar las redes sociales y que tener en cuenta sobre la mensajería gratuita.
Abril	Conexiones inalámbricas o Wifi.	Informar a los empleados los riesgos a que nos vemos expuestos al utilizar una red inalámbrica sin protección o desconocida.
Mayo	Backus de los datos	por qué?, ¿y para qué? Es importante respaldar nuestra información.
Junio	Tipos de amenazas	Dar a conocer los tipos de amenazas cibernéticas.
Julio	Recursos informáticos	Monitoreo de los recursos informáticos en el Instituto.
Agosto	One drive	Concientizar donde guardar la información para que siempre esté disponible.
Septiembre	Ingeniería social	Concientizar en donde se habla y delante de quién.
Octubre	Estaciones de trabajo desatendidas	Dar a conocer lo que se puede hacer, cuando se deja la estación de trabajo desatendida.
Noviembre	Control de acceso	Control de acceso a la red y la seguridad en las contraseñas.
Diciembre	Lo aprendido	Concurso que hemos aprendido de seguridad de la información y premiación.

MEDICIÓN DE CONTROLES

Tratamiento	Nivel de Implementación
Renovación de antivirus	99% se implementó, faltan muy pocos por actualizar la nueva versión (equipos trabajo en casa)
Lineamiento de seguridad para servidores y estaciones de trabajo.	100% Los controles están implementados
Política de seguridad para dispositivos móviles.	100% Los controles están implementados.
Prestación de servicios para la administración de vulnerabilidades	100% se implementó, pero no se hacen análisis de ética hacking
Política para control de puertos USB.	100% se implementó y se monitorea
Elaboración de estándar asignación cuentas de usuario y gestión de privilegios.	97% se implementó, pero los resultados no son óptimos algunos usuarios mal creados falta información
Elaboración de instructivo envío de información confidencial de forma segura con herramientas de encriptación.	10% no se ha implementado, ni se monitorea
Procedimiento estándar identificación y Autenticación de cuentas de usuario.	100% se implementó y se monitorea
Implementar controles físicos para ingresar al Data Center.	100% se implementó y se monitorea
Programar mantenimiento preventivo de los servidores.	0% No se ha implementado
Capacitar a los del área de soporte técnico sobre la infraestructura de comunicación y data center.	0% No se ha implementado

CONCLUSIONES

- Al realizar la gestión de riesgos se comienza desde la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, igualmente se analiza la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

- Se concluye que para hacer una gestión de riesgos se debe asegurar que los objetivos, políticas y procesos de TI y conocer la importancia de cada uno de los activos de tecnología que soportan nuestra infraestructura tecnológica.

- Con la gestión de riesgos que se realizó, se logrado identificar los riesgos críticos de TI que pueden ser una amenaza, se realiza la implementación de controles que evalúan las distintas situaciones de riesgos.

SEGUIMIENTO

INDEPORTES ANTIOQUIA revisará anualmente la gestión del riesgo Revisando los activos de información y valorando los riesgos de los mismos, iniciando desde la revisión de la política de Seguridad y Privacidad de la Información. Para lo anterior se seguirán los lineamientos de MINTIC, la Guía para la administración del riesgo y el diseño de controles en entidades públicas, Función Pública y la norma ISO 27001.

El seguimiento y monitoreo al Plan de Tratamiento de Riesgos estará a cargo de la Oficina de Sistemas e Informática. Esta Oficina evalúa el desarrollo y cumplimiento de las acciones contempladas para prevenir o mitigar los riesgos identificados en los procesos establecidos en el alcance instrumento para hacer seguimiento y monitoreo al riesgo de los activos de información.