fodesep
Fondo de desarrollo de la educación superior
Vinculado al Ministerio de Educación Nacional

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-FODESEP 2022

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GESTIÓN DE RIESGOS – FODESEP

1. *Antecedentes*

El FODESEP realizó una modernización y renovación a la plataforma tecnológica en todos los casos y durante años, buscando una mejora eficaz, eficiente y efectiva para los procesos de la Entidad y como estrategia de apoyo al desarrollo e implementación de su sistema Informático y de información buscando cumplir con su misión y visión.

Dado lo anterior, se debe disminuir los riesgos y siniestros informáticos que se presenten en la entidad, como también reducir la posibilidad de ocurrencia.

En el último año FODESEP registro un incidente informático, debido a que un disco duro de un servidor completo su máximo de almacenamiento y en el momento en el que se quiso ampliar la capacidad de los discos, el servidor por su configuración de RAID presento un error y se desconfiguró la solución raid. Dado lo anterior, no se pudo realizar la instalación del disco duro nuevo y se revirtió todo lo que se había realizado, para que el servidor quedara en su estado anterior.

Teniendo en cuenta que el FODESEP es una entidad vinculada al Ministerio de Educación, donde se adoptara el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno Digital, haciendo necesario poner en marcha un Plan de Seguridad de la Información donde se deben “identificar” aquellos riesgos, que colocan inestable los Servicios Tecnológicos institucionales y la continuidad de estos, se debe orientar los pasos a seguir en caso de presentarse un incidente de estos, que permitirá recuperar la funcionalidad de la plataforma tecnológica, garantizando la continuidad de las operaciones de la Entidad en el cumplimiento misional.

2. *Objetivos*

- Asociar la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información
- Gestionar los riesgos de Seguridad de la información teniendo en cuenta los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad)
- Reconocer las situaciones de riesgo que pueden afectar la infraestructura informática, las actividades que minimizan la materialización de dichos imprevistos y poder actuar en fin de la continuidad de la operación de la plataforma tecnológica Institucional.
- Garantizar la resiliencia en la entidad.
- Estimar las posibles situaciones que generan los riesgos.

- Identificar las actividades que actualmente mitigan la presencia de los riesgos estimados.
- Establecer la continuidad o nuevas acciones para retomar el curso normal de operación en caso de presentarse los riesgos valorados.
- Brindar respuesta rápida y oportuna para dar continuidad a las operaciones que componen la infraestructura tecnológica.
- Procurar que la restauración de los servicios de informática y tecnología sean con un impacto mínimo de costo / pérdida para la entidad.

3. *Justificación*

Dado a que todos los días tenemos nuevas tecnologías y mercados cada vez más competitivos en el día a día, lo anterior nos vuelve más dependientes de estas calidades de manejo de riesgos, servicios y la continuidad del negocio, convirtiendo estas herramientas en una forma transcendental de sostener la continuidad del negocio en los mejores niveles de disponibilidad, confiabilidad, rendimiento y funcionalidad.

Los procedimientos y otros documentos que actualmente son parte del proceso de tecnología del FODESEP, pueden mitigar una parte del riesgo, pero estos sólo son de aplicabilidad transitoria y no asisten de forma específica una solución válida en la atención de un riesgo a la plataforma Informática.

En caso de existir un accidente informático en la interrupción de cualquiera de los servicios informáticos, en alguno o varios de sus dispositivos, ya sea de tipo eléctrico, hardware, software y demás; conllevando a un impacto financiero, mala imagen, entre otros más factores que causarían posibles pérdidas, ocasionando el cese de actividades en la continuidad del negocio.

Al tener una identificación de los Riesgos para la Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno Digital, permitirá cubrir costos innecesarios en materiales de los activos de la entidad en caso de una calamidad, y servirán para recuperar el negocio en lo más preciado que es su información, evitando la pérdida de esta.

4. *Identificación de Riesgos*

En virtud de lo planteado en la guía, la identificación del riesgo se hace con base en causas identificadas para los procesos, dichas causas pueden ser internas o externas, según lo que haya identificado la Entidad a través del Contexto estratégico.

En esta parte es importante la participación del personal elegido para la implementación del MSPI, en la mesa interdisciplinaria en la cual se revisan los procesos, haciendo parte de la

identificación de los riesgos de seguridad, para los procesos identificados como críticos dentro del planteamiento del MSPI.
Inicia con la definición de algunos términos que son necesarios dentro del empleo de esta metodología, son los relacionados a continuación:

- Proceso.
- Objetivo del Proceso.
- Identificación de Activos.
- Riesgo.
- Causas (Amenazas y Vulnerabilidades).
- Descripción del Riesgo.
- Efectos de la materialización del Riesgo.

Luego se debe realizar la clasificación de los riesgos, para el caso del FODESEP se hará la identificación de "**Riesgos de Tecnología**", teniendo en cuenta los pilares de la seguridad de la información:

- Disponibilidad
- Confidencialidad
- Integridad

5. ANÁLISIS DE RIESGOS

A continuación, se muestran una sucesión de etapas propuestas para la Generación del análisis de riesgos de las Entidades, basadas la norma ISO 27005.

5.1. IDENTIFICACIÓN DEL RIESGO

La intención de la identificación del riesgo es establecer que podría pasar en caso de que suceda una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida. Las siguientes etapas deberían recolectar datos de entrada para esta actividad.

5.2. IDENTIFICACIÓN DE LOS ACTIVOS

Conforme a la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se deberá llevar a cabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo. Para realizar esta identificación es necesario revisar la guía de gestión de activos adjunta al MSPI.

5.3. IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza tiene el potencial de causar daño a activos como: La información, procesos y sistemas por lo tanto las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas, por ellos es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo.

Las amenazas pueden afectar a varios de un activo y en algunos casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

A continuación, se describen una serie de amenazas comunes.
D= Deliberadas, A= Accidentales, E= Ambientales

Para los riesgos tecnológicos que se identificaran, se tendrá en cuenta las probables amenazas comunes y las amenazas humanas que apliquen al FODESEP.

- **Fuentes de amenazas comunes**

TIPO	AMENAZA	ORIGEN
PERDIDA DE LOS SERVICIOS ESENCIALES	Fallas en el sistema de suministro de aire acondicionado	D A
	Perdida de suministro de energía	A
	Falla en la capacidad de almacenamiento	D A
	Falla en equipo de telecomunicaciones	D A
Compromiso de la información	Hurto de equipo	A
	Manipulación con hardware	A
	Manipulación con software	A
Fallas técnicas	Fallas del equipo	A E
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	D A

TIPO	AMENAZA	ORIGEN
Acciones no autorizadas	Uso no autorizado del equipo	D A
	Uso de software falso o copiado	D A
	Corrupción de los datos	D A
	Procesamiento ilegal de datos	D A
	Copia fraudulenta del software	D A

- **Fuentes de amenazas humanas**

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación	• Penetración en el sistema • Manipulación en el sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	• Asalto a un empleado • Chantaje • Observar información reservada • Uso inadecuado del computador • Fraude y hurto • Soborno de información • Ingreso de datos falsos o corruptos • Interceptación • Código malicioso

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
		• Venta de información personal • Errores en el sistema • Intrusión al sistema • Sabotaje del sistema • Acceso no autorizado al sistema.

5.4. IDENTIFICACIÓN DE CONTROLES EXISTENTES

Algunos controles que se van a tener, para evitar riesgos o amenazas a la plataforma tecnológica son:

- Borrador POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.
- Realizar una vez al año como mínimo auditorías internas, para control de licenciamiento institucional, uso de Internet, y demás, en cumplimiento de la Política de seguridad y privacidad de la información.
- control de DERECHOS DE AUTOR de licenciamiento institucional.
- Bloqueo de permisos en el directorio activo en la red interna del FODESEP.

5.5. IDENTIFICACIÓN DE LAS VULNERABILIDADES

Lo que nos aplica y se identificaran vulnerabilidades en el área “Hardware, software y equipos de comunicaciones”.

Vulnerabilidades identificadas en el proceso de Tecnología y métodos para la valoración de la misma.

TIPO DE ACTIVO	***VULNERABILIDADES***	***AMENAZAS***
SERVIDOR	ACCESO A INTERNET	HACKING
SOFTWARE CYGNUS	VERSIONAMIENTO 2008	DAÑO EN BDE INFORMACION
INFORMACION EQUIPOS	PERDIDA DE INFORMACION	BORRADO ACCIDENTAL DE INFORMACION
DAÑO EQUIPOS	DAÑO POR GOLPES	MOVILIZACION DE PORTATILES

6. Pasos para análisis del Riesgo

Impacto:

- Activo (¿qué se trata de proteger?)
- Amenaza (¿que se teme que suceda?)

Probabilidad:

- Vulnerabilidad (¿cómo se puede ocurrir la amenaza?)
- Mitigación (¿cómo se reduce actualmente el riesgo?)

Siguiendo el "Estándar AS/NZS 4360 de Análisis de Riesgos de la Metodología del Ministerio de Comunicaciones (Gobierno Digital - MINTIC).

1. Establecer el contexto: Administración de riesgos
2. Identificar Riesgos: Los expuestos en este documento son de Tipo Tecnológico.
3. Analizar Riesgos

- Aplicar las medidas cualitativas de Impacto
- Aplicar las medidas cualitativas de probabilidad

4. Evaluar Riesgos:

- Comparar contra criterios
- Establecer prioridades de riesgo

5. Tratar Riesgos: Aplicar los pasos dados en el estándar AS/NZS 4360 Matriz de Análisis de Riesgo Cualitativo
6. Aplicación de la Matriz de Análisis de Riesgo Cualitativo

7. Identificación y Análisis de Riesgos Informáticos

TIPO ACTIVO	PROBABILIDAD / VULNERABILIDAD	IMPACTO / AMENAZA	ACCIONES PREVENTIVAS/CORRECTIVAS	EJECUCION
SERVICIO DE INTERNET, SERVIDORES, SWITCH, ROUTER, REDES LAN, Wifi. Ataques a la plataforma informática	Los ataques pueden ser internos o externos por: Deficiencia o falta de una Política de Seguridad Informática institucional definida. Correctamente para el uso los Sistemas Informáticos del FODESEP. Herramientas de Seguridad Perimetral poco eficaces en hardware y software en la construcción e implantación de Políticas eficaces en el FODESEP.	Accesos no autorizados por parte de "delincuentes informáticos" u otros con pretensiones de causar daños potenciales a la Red informática del FODESEP y datos contenidos en estos, mediante ataques a los sistemas que componen la Plataforma Informática.	Mantener activa y actualiza la solución de antivirus. Firewall actualizado y con políticas restrictivas. Procedimiento Instalación de software y servicios.	Octubre 2022

SERVIDORES INSTITUCIONALES Pérdida de información en los Servidores	Falta de mantenimiento preventivo y correctivo a los Sistemas de: equipos Servidores. Sistema eléctrico regulado UPS´s y a la red LAN. Servidores que componen la Planta Informática. Desconocimiento de los Ingenieros Por desconfiguración en equipos. Ausencia de un sistema de Backup´s Falta tercerizar los servicios en la NUBE Soportes poco idóneos. Ausencia de Políticas de Seguridad Informática para los Servidores. Desarrollos inadecuados de aplicativos o implementaciones mal realizadas. Obsolescencia.	Daños físicos o lógicos en los servidores institucionales. Caída de la red LAN Fallo en el Fluido eléctrico regulado por UPS Propagación de virus o programas basura como SPAM Daños en aplicativos y/o Base de datos. Daños físicos en discos duros. Alteración de los desarrollos de los aplicativos. Caídas del servicio de Internet	Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológica. Solución de Backus automatizada y en la nube. Política de Seguridad aplicada. Exigir estándares de desarrollo y acuerdos de confidencialidad. Procedimiento Instalación de software y servicios. Copia de respaldo (backup) y restauración de la información de los equipos de cómputo. Administración de claves de servidores y equipos. Actualizaciones técnicas a los servidores,	MAYO 2022

TIPO ACTIVO	PROBABILIDAD / VULNERABILIDAD	IMPACTO / AMENAZA	ACCIONES PREVENTIVAS/CORRECTIVAS	EJECUCION
EQUIPOS ELECTRÓNICOS Y HARDWARE. Falla de equipos electrónicos y hardware.	Ausencia de Políticas claras y definidas en el uso correcto de equipos electrónicos y de Hardware. Planes de Mantenimiento preventivo y correctivo anuales a la Planta Informática del FODESEP. Adecuación completa de una red eléctrica regulada en el 100% del FODESEP que cumpla con normas vigentes para la protección entre otros de equipos electrónicos.	Estas se pueden dar por: Cumplimiento de vida útil de un equipo de cómputo. Uso continuo de equipo electrónico. Falta de Mantenimientos Preventivos y Correctivos No se cuenta con una red eléctrica regulada o completa. Ineficiente cantidad de UPS Mal uso por parte de los responsables de los equipos	Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológica. Política de Seguridad aplicada. Copia de respaldo (backup) y restauración de la información de los equipos de cómputo.	MAYO 2022

TIPO ACTIVO	PROBABILIDAD / VULNERABILIDAD	IMPACTO / AMENAZA	ACCIONES PREVENTIVAS/CORRECTIVAS	EJECUCION
UPS Y RED REGULADA. Fallas en el suministro de Energía Eléctrica Regulada o UPS (Sistemas de Poder Ininterrumpido) y Red Alambrada CAT 7a	Por falta de mantenimiento preventivo y correctivo a la Planta de UPS actuales y el sistema de tomas eléctricas de los puestos de trabajo. Políticas no existentes o poco claras en su uso. Inestabilidad de la UPS por sobrecarga. Deficientes conexiones en tomas eléctricas reguladas.	Se puede dar por: Deficiencia de UPS para mantener los servicios por un tiempo razonable en los equipos. Sistema de UPS poco confiables Conexiones inadecuadas en tomas eléctricas de puestos de trabajo Malas conexiones de las UPS Niveles de carga eléctrica mayores a los soportados por la Red Eléctrica o las UPS Ausencia de Línea a Tierra (GND) Calidad del cableado eléctrico ineficiente o poco confiable.	Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológica. Política de Seguridad aplicada. Adquisición de planta eléctrica.	MAYO 2022

TIPO ACTIVO	PROBABILIDAD / VULNERABILIDAD	IMPACTO / AMENAZA	ACCIONES PREVENTIVAS/CORRECTIVAS	EJECUCION
TELEFONÍA IP. Caídas del servicio telefónico IP	Por falta de: Mantenimiento a los equipos del servicio. Soporte al aplicativo telefonía IP y sus funcionalidades. Obsolescencia.	Se puede dar por: Caída del Servidor. Fallo en la Fibra Óptica del proveedor o en los equipos Router del operador. Desconexiones de Red en los teléfonos IP. Fallos en Red LAN. No renovación de contrato de proveedor de servicio del canal dedicado de internet.	Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológica. Actualización de software telefonía IP. Tener un servicio de internet contingente con otro operador.	MAYO 2022

TIPO ACTIVO	PROBABILIDAD / VULNERABILIDAD	IMPACTO / AMENAZA	ACCIONES PREVENTIVAS/CORRECTIVAS	EJECUCION
RED DE DATOS Fallos de la Red de Datos por una mala instalación o cortos presentados en esta.	Por falta de: Ausencia de una política de Red de Datos. Certificación de la Red institucional. Maquillaje o identificación de puntos de red. Organización correcta de puntos de datos en el Centro de Datos. Mantenimiento a los dispositivos de redes como Switch. Reorganización del cableado de datos Certificación de la red de datos Redistribución de puntos	Se puede dar por: Corto en Puntos de Datos. Congelamiento de la red por daños. Dispositivos Switch en mal estado. Cables en mal estado. Deficiente distribución por pisos. Pachtcord o Crossover hechos manualmente. Manipulación inadecuada de los cables.	Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológica. Política de Seguridad aplicada. Tener un servicio de internet contingente con otro operador.	MARZO 2022
PÁGINA WEB INSTITUCIONAL Manipulación indebida de los archivos fuentes y	Pérdida de Control en el manejo de la página WEB. Accesos no autorizados Manipulación de los datos	No habría control total de los archivos fuentes y las bases de datos	Acuerdos de confidencialidad. Solución de Backup´s (diarios, semanales). Perfil de usuario de administración.	ABRIL 2022

TIPO ACTIVO	PROBABILIDAD / VULNERABILIDAD	IMPACTO / AMENAZA	ACCIONES PREVENTIVAS/CORRECTIVAS	EJECUCION
bases de datos de la página WEB				
INFORMACIÓN INSTITUCIONAL Sustracción no autorizada de Datos e información institucional	Puede ocurrir por: Falta de lineamientos en cuanto a responsabilidades del manejo de la información. Controles poco eficientes en accesos no autorizados - Exceso de confianza en el manejo de las responsabilidades	Se puede dar por: Personal no autorizado tiene acceso no autorizado a los sistemas informáticos, equipos de cómputo, servidores, archivos importantes, lo que convierte la Plataforma Tecnológica en algo muy sensible a pérdidas, alteración, daño o robos de información.	Política de Seguridad aplicada. Firewall con políticas de seguridad activas. Administración controlada de la red de datos. Procedimiento Instalación de software y servicios. Copia de respaldo (backup) y restauración de la información de los equipos de cómputo. Administración de claves de servidores y equipos.	ABRIL 2022
HARDWARE Y SOFTWARE Daños en equipos y/o el software por el ataque de virus informáticos	Puede ocurrir por: Falta de políticas en el uso de Software Ausencia de un programa antivirus en los equipos Deficiente administración del Antivirus Actualizaciones no realizadas Desactivación del antivirus	Propagación de programas o rutinas dañinas que afecten los sistemas informáticos.	Política de Seguridad aplicada. Solución de antivirus actualizada. Firewall actualizado y con políticas. Procedimiento Instalación de software y servicios.	ABRIL 2022

TIPO ACTIVO	PROBABILIDAD / VULNERABILIDAD	IMPACTO / AMENAZA	ACCIONES PREVENTIVAS/CORRECTIVAS	EJECUCION
SEGURIDAD PARA EL INGRESO, MANEJO Y DISPOSICIÓN DE INFORMACIÓN EN EQUIPOS ASIGNADOS Fallas del manejo de claves de acceso y manejo de equipos	Malversación o pérdida de información institucional causada por préstamo de las claves de acceso. Dificultad para consultar, manejar y disponer de la información por perdida de las claves de acceso. Retrasos en la gestión institucional por los reprocesos de reasignación y definición de nuevas claves de acceso para disponer de la información	Se puede dar por: Ausencias temporales de los servidores (enfermedad, accidente, encargos de puestos de trabajo, retiro temporal por sanción disciplinaria). Ausencias definitivas de los servidores (finalización de la vinculación laboral, renuncias, abandono del cargo, traslado definitivo de puesto) Deficiencias en el manejo de las claves de acceso por olvido, manipulación o intentos fallidos.	Procedimiento de contingencia para atender las ausencias justificadas o injustificadas. Procedimiento Administración de claves de servidores y equipos.	ABRIL 2022

TIPO ACTIVO	PROBABILIDAD / VULNERABILIDAD	IMPACTO / AMENAZA	ACCIONES PREVENTIVAS/CORRECTIVAS	EJECUCION
INFRAESTRUCTURA INFORMÁTICA Sabotaje / vandalismo	Deficiencias en el control de ingreso no autorizados a los Centros de Datos o equipos de red ubicados en diferentes sitios a este y que carecen de seguridad, lo que pueden ser manipulables por cualquiera.	El Centro de Datos se encuentra dispuesto en dos espacios físicos diferentes en la entidad, en razón a esto, se dificulta controlar el acceso de personas que puedan alterar el normal funcionamiento de los sistemas informáticos.	Se tiene un control de acceso al centro de datos, se debe tener mínimo configurada el uso de dos tarjetas inteligentes, asignadas a 2 funcionarios para el acceso diferentes claves de servidores y equipos. Respaldo del centro de datos externo de la sede principal del FODESEP, donde esta actualmente el centro de datos principal.	MAYO 2022

TIPO ACTIVO	PROBABILIDAD / VULNERABILIDAD	IMPACTO / AMENAZA	ACCIONES PREVENTIVAS/CORRECTIVAS	EJECUCION
INFRAESTRUCTURA INFORMÁTICA Desastres naturales / Conflagraciones, inundaciones, movimientos telúricos que afecten la infraestructura informática.	El FODESEP, no está exento de que se pueden presentar cortos en las tomas eléctricas, por ende, recalentamiento en equipos, o hechos más graves como conflagraciones que afecten los equipos y redes informáticos. Los equipos de cómputo, la red eléctrica regulada, la red LAN (canaletas) puede sufrir daños, causados por inundaciones al presentarse rupturas en la tubería del agua. La presencia de los movimientos telúricos es alta e impredecible, lo que provocaría que en el FODESEP se presente catástrofe en la infraestructura física, de acuerdo a estudio realizado por la Universidad Nacional	Incendios, inundaciones, movimientos telúricos que afecten la infraestructura informática provocando daños en la misma (perdida de información, daños en equipos que generen parálisis en la gestión institucional)	UN Plan de contingencia con solución de Backups en la nube. Copia de respaldo (backup) y restauración de la información de los equipos de cómputo. Respaldo del centro de datos externo de la sede principal del FODESEP, donde está actualmente el centro de datos principal.	ABRIL 2022

TIPO ACTIVO	PROBABILIDAD / VULNERABILIDAD	IMPACTO / AMENAZA	ACCIONES PREVENTIVAS/CORRECTIVAS	EJECUCION
	donde la edificación principal no cumple con normas de sismo resistencia, afectando por ende la infraestructura informática			

EVALUACIÓN DE RIESGO

Esta se hace de manera cualitativa generando una comparación en la cual se Presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz denominada "Matriz de Calificación, Evaluación y respuesta a los Riesgos", con la cual la guía presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos anteriormente, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra en la siguiente imagen:

Ilustración 3 "Matriz de Calificación, Evaluación y respuesta a los Riesgos"

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Fuente: Guía de Riesgos DAFP

Teniendo en cuenta los pasos mencionados anteriormente, y las herramientas entregadas por la guía, se presenta a continuación el análisis de uno de los riesgos de Seguridad de la Información identificados anteriormente:

Matriz de análisis de riesgo cualitativo

Probabilidad	**Impacto**				
	Insignificante 1	Menores 2	Moderados 3	Mayores 4	Catastróficas 5
A (casi certeza)	A	A	E	E	E
B (probable)	M	A	A	E	E
C (moderado)	B	M	A	E	E
D (improbable)	B	B	M	A	E
E (raro)	B	B	M	A	A

B: Bajo **M:** Moderado **A:** Alto **E:** Extremo

Aplicación Matriz y calificación de los riesgos

Riesgo	**Probabilidad**	**Impacto**	**Calificación**
Servicio de Internet, Servidores, Switch, Router, redes LAN, Wifi. Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia BAJA	D	2	**B**
Pérdida de información en los Servidores Evaluado el riesgo y lo que actualmente ha hecho se ha hecho para reducir este, es de ocurrencia ALTA	B	2	**A**
Falla de equipos electrónicos y Hardware Evaluado el riesgo y lo que actualmente ha hecho se ha hecho para reducir este, es de ocurrencia MODERADO	C	2	**M**

Riesgo	Probabilidad	Impacto	Calificación
Fallas en el suministro de Energía Eléctrica Regulada o UPS (Sistemas de Poder Ininterrumpido) Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia ALTA	B	3	**A**
Caídas del Servicio Telefónico IP Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia MODERADO	C	2	**M**
Fallos de la Red de Datos Evaluado el riesgo y lo que se ha hecho para reducir este, es de ocurrencia ALTA	C	3	**A**
Página WEB institucional Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia ALTA	C	3	**A**
Robo común de Datos e información institucional Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia MODERADO	B	2	**M**
Equipos de virus informáticos Evaluado el riesgo y lo que se ha hecho para reducir este, es de ocurrencia MODERADO	C	2	**M**
Fallas de personal "clave" de Informática Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia ALTO	B	3	**A**
Sabotaje / vandalismo Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia ALTO	B	2	**A**

Riesgo	Probabilidad	Impacto	Calificación
Conflagraciones, inundaciones, movimientos telúricos que afecten la infraestructura informática. Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia ALTO	B	3	**A**

https://www.pmg-ssi.com/2017/05/iso-27001-plan-de-tratamiento-de-riesgos-de-seguridad-de-la-informacion/

Referencias: Ministerio de Comunicaciones y Gobierno en Línea de Colombia Guía No. 7 Gestión de Riesgos