ESE Hospital Regional de Duitama

Plan de servicio: Plan De Tratamiento De Riesgos De Seguridad De La Información

	ESE Hospital Regional de Duitama **Proceso:** Gestión de la Información **Subproceso:** Tecnologías de la información **Plan de servicio:** Plan De Tratamiento De Riesgos De Seguridad De La Información	**Código** **Fecha** **Versión**

Estratégico	Misional	Apoyo	Evaluación

Objetivo

Administrar los riesgos relacionados con la seguridad de la información mediante su identificación, análisis, control y evaluación, con base en criterios de confidencialidad, integridad y disponibilidad de los activos de información y la infraestructura crítica de la E.S.E. Hospital Regional de Duitama.

Responsable

Líder Tecnología De La Información (Tecnologías de la Información)

Alcance

A través del análisis, control y evaluación de los riesgos, se busca mitigar, reducir o eliminar la probabilidad e impacto de incidentes de seguridad de la información. Este documento aplica a los activos de seguridad de la información de la **E.S.E. Hospital Regional de Duitama** y sus sedes anexas.

Introducción

Este documento se enfoca en la gestión y tratamiento de los riesgos de **seguridad y privacidad de la información**, alineado con el **Modelo de Seguridad y Privacidad de la Información**. Se detallan los riesgos identificados en el área de **Tecnologías de la Información**, abarcando tanto la infraestructura crítica como los servicios tecnológicos.

Se han identificado seis riesgos clave, los cuales están relacionados con la interrupción de procesos administrativos y la prestación de servicios de salud debido a:

- Fallas en los equipos de cómputo
- Problemas en los servicios tecnológicos
- Deficiencias en los centros de cableado
- Ataques cibernéticos
- Uso inadecuado del software
- Posible alteración de información sensible

Para cada uno de estos riesgos, se establecen controles y tratamientos correctivos o preventivos, los cuales permiten monitorear, dar seguimiento y evaluar su mitigación progresiva. Esto da lugar a un **plan de implementación** que será ejecutado durante la **vigencia 2025**.

Considerando los objetivos institucionales y la necesidad de reducir el impacto de los riesgos, para **2025** se ha priorizado la intervención del riesgo de mayor nivel: la **posible encriptación o secuestro de la información digital** en las bases de datos de los sistemas de información y archivos de los equipos de cómputo.

Responsables

ÁREA O ROL INSTITUCIONAL	RESPONSABILIDADES
Directivos de la Entidad	Encargados de la aprobación de los proyectos de inversión en temas de seguridad y privacidad de la información.
Contro Interno, Planeación Institucional y Gestión de Calidad.	Responsables de auditorias, control y seguimiento al tratamiento de riesgos de seguridad de la información.
Lider de Tecnologías de la Información	Responsables del tratamiento de los riesgos de seguridad de la información.
Responsable de la seguridad Institucional	
Equipo de Tecnologías de la Información	
Líderes y Coordinadores institucionales	

Colaboradores y/o funcionarios de la entidad	Apoyan y adoptan la gestión de buenas prácticas de seguridad y privacidad de la información.
Proveedores	Adoptan las políticas institucionales de seguridad y privacidad de la información.

Marco Legal y/o Teórico

Políticas técnicas de seguridad de la Información Función Pública, 2020: La declaración de la Política de Seguridad de la Información institucional busca proteger los activos de información (grupos de valor, información, procesos, tecnologías de información incluido el hardware y el software), mediante el establecimiento de lineamientos generales para la aplicación de la seguridad de la información en la gestión de los procesos internos, bajo el marco del Modelo Integrado de Planeación y Gestión, consolidada en los procedimientos, guías, instructivos y publicaciones, así como la asignación de roles y responsabilidades.
Decreto 103 de 2015, 2019: Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.
Decreto 1494 de 2015, 2019: Por el cual se reglamenta parcialmente la Ley 171de 2014 y se dictan otras disposiciones.
Decreto 1008, 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Ley 1712 de 2014, 2018: Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
Decreto 2573 de 2014, 2018: Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones.
Decreto 1377 de 2013, 2018: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 2609 de 2012, 2017: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley estatutaria 1581 de 2012, 2017: Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
Ley 1474 de 2011, 2017: Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Ley 527 de 1999, 2015: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Norma técnica colombiana NTC - ISO/IEC 27001, 2013: Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa.
Norma NTC/ISO 27002, 2013: Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.
Norma NTC / ISO 31000, 2009: Gestión de Riesgo, Principios y Directrices.

Diagnostico y/o situación actual

En el modelo de seguridad y privacidad de la información, el la FASE 1: Diagnostico, se tiene el análisis de la situación actual de la entidad, con la metodología para la identificación de los activos de la información y la infraestructura critica. El Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información en un producto que enfatiza su contenido para el control y tratamiento de los riesgos.

Definiciones

Activo: Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización - Servicios web -Redes - Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital.
Apetito de riesgo: es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
Análisis de Riesgo: Uso sistemático de la información para identificar fuentes y estimar el riesgo (Guía ISO/IEC 73:2002).
Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.
Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.
Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar su importancia.
Factor de riesgo: Agente ya sea humano o tecnológico que genera el riesgo.
Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
Integridad: propiedad de exactitud y completitud. Mapa de riesgos: documento con la información resultante de la gestión del riesgo.
Nivel de riesgo: es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.
Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
Riesgo: Efecto de la incertidumbre sobre el cumplimiento de los objetivos.
Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
Tolerancia del riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
Tratamiento del riesgo: Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.
Valoración del riesgo: Proceso de análisis y evaluación del riesgo.
Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

Recursos, Materiales, Insumos y Equipos

El presente documento es un producto del programa institucional "Modelo de Seguridad y Privacidad de la Información". Este documento se utiliza como insumo para ver el estado actual de la entidad en relación a seguridad y privacidad de la información y de esa forma determinar los riesgos inherentes a Seguridad Digital.

Desarrollo

1. **MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

1.1 SITUACIÓN ACTUAL

En el modelo de seguridad y privacidad de la información, el la FASE 1: Diagnostico, se tiene el análisis de la situación actual de la entidad, con la metodología para la identificación de los activos de la información y la infraestructura critica. El Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información en un producto que enfatiza su contenido para el control y tratamiento de los riesgos.

2. **TRATAMIENTO DE RIESGOS DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

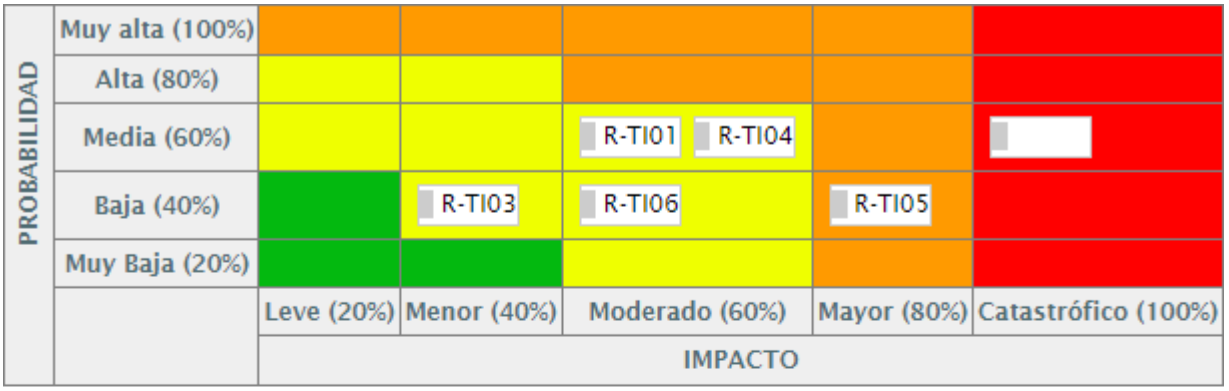
La entidad, integrando el Modelo de Seguridad y Privacidad de la Información (MSPI) con el objetivo de implementar un Sistema de Gestión de Seguridad de la Información, gestiona este documento alineado con la fase de implementación del MSPI.

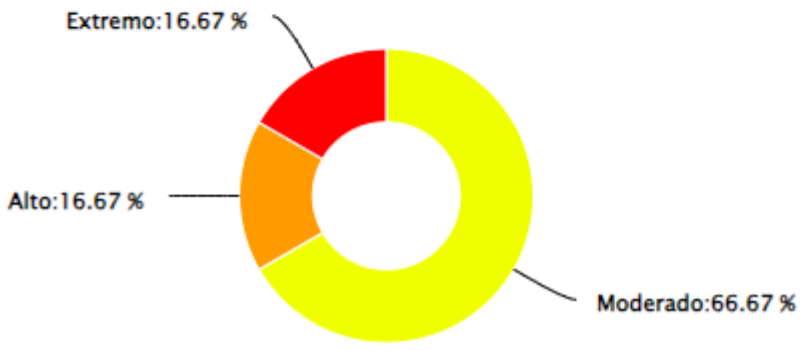
1. **RIESGOS**

A través del software institucional Almera, en el cual se gestionaron los riesgos de seguridad y privacidad de la información, se puede obtener un análisis resumido de los seis (6) riesgos relacionados a los activos de la información y a la infraestructura critica, los cuales son:

Unidad de riesgo	Cod Riesgo	Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Controles
Tecnologías de la información	R-TI01	Posibilidad de afectación en la atención de los servicios de salud e interrupción en la ejecución de actividades administrativas.	Media (60%)	Moderado (60%)	Moderado	3
Tecnologías de la información	R-TI02	Posibilidad de encriptación o secuestro de la información digital de las bases de datos de los sistemas de información y archivos de los equipos de cómputo.	Media (60%)	Catastrófico (100%)	Extremo	1
Tecnologías de la información	R-TI03	Posibilidad de uso inadecuado del software e información digital institucional.	Baja (40%)	Menor (40%)	Moderado	2
Tecnologías de la información	R-TI04	Posibilidad de falla en los servicios tecnológicos de la red de datos, internet, telefonía y correos electrónicos.	Media (60%)	Moderado (60%)	Moderado	2
Tecnologías de la información	R-TI05	Probabilidad de incidentes en los centros de datos de la entidad.	Baja (40%)	Mayor (80%)	Alto	1
Tecnologías de la información	R-TI06	Posibilidad de alteración de información sensible debido a la manipulación de los sistemas de información por intereses de terceros o particulares	Baja (40%)	Moderado (60%)	Moderado	2

Los cuales generan una matriz de calor, en la cual se relaciona la probabilidad junto al impacto para determinar el nivel del riesgo.





Se puede determinar que los 6 riesgos están organizados de la siguiente forma:

	RIESGO			
Extremo	R-TI02			
Alto	R-TI05			
Moderado	R-TI03	R-TI06	R-TI01	R-TI04
Bajo	NINGUNO			

B. CONTROLES Y/O TRATAMIENTO

Cada uno de los riesgos identificados tiene una serie de controles cuyo objetivo tienen mitigar la probabilidad o mitigar el impacto.

Controles de los Riesgos de Seguridad y Privacidad de la Información

Nombre	Código control	Descripción	Clase	Tipo	Mitiga Probabilidad	Mitiga Impacto	Estado	Responsable(s) Aplicación	Forma de ejecución
Configuración de una red de datos en anillo redundante con asignación de VLAN para mejora del trafico de información.	01	La red de datos institucional debe ser configurada con una topología en anillo redundante que permita la generación de fallas sin que afecte totalmente los servicios de la entidad, asignado redes virtuales o VLAN para mejora del tráfico de la información y conexión entre los equipos y servidores.	Actual	Correctivo	No	Si	Vigente	Líder Tecnología De La Información (Tecnologías de la Información)	Manual
Ejecución del mantenimiento preventivo a los equipos tecnológicos de la entidad.	02	Mediante la ejecución del mantenimiento preventivo programado, se minimiza la probabilidad de errores en los equipos tecnológicos, al poder intervenir o corregir un problema antes de su aparición.	Actual	Preventivo	Si	No	Vigente	Líder Tecnología De La Información (Tecnologías de la Información)	Manual
Actualización de la infraestructura de hardware.	03	Mediante la baja y reposición de infraestructura crítica tecnológica, se puede evitar la generación o aparición de problemas relacionados a la obsolescencia de los equipos, teniendo en cuenta, que con el avance tecnológico, cada vez se requieren mejores especificaciones de hardware y software.	Actual	Preventivo	Si	No	Vigente	Líder Tecnología De La Información (Tecnologías de la Información)	Manual
Implementación de una seguridad cibernética empresarial apoyados de una empresa con experiencia en combatir ataques de ciberdelincuentes.	01	La entidad debe realizar la inversión en una plataforma de seguridad empresarial que proteja la información y la infraestructura crítica con una empresa que tenga experiencia en este sector y configure las políticas de seguridad y sea la principal responsable ante incidentes de seguridad.	Actual	Correctivo, Detectivo	Si	Si	Vigente	Líder Tecnología De La Información (Tecnologías de la Información)	Manual
Capacitación inducción y re inducción de los usuarios finales que hacen uso de los sistemas de información.	01	Algunos de los errores que se presentan en los sistemas de información se debe a la ausencia de conocimiento, fortalecimiento y seguimiento de este, en relación al uso y dominio de los sistemas de información. El área de tecnologías de la información, realiza una capacitación inicial en la cual se despejan las dudas, sin embargo, no se realiza un seguimiento al personal nuevo que ingresa sobre dudas e inquietudes sobre la gestión de actividades.	Actual	Preventivo	Si	No	Vigente	Líder Tecnología De La Información (Tecnologías de la Información)	Manual
Contratación de actualización, mantenimiento y soporte de los sistemas de información.	02	La entidad tiene varios sistemas de información, es importante tener contrato de actualización, soporte y mantenimiento de los mismos, con el objetivo de solucionar errores y tener un apoyo en el caso de tener dudas e inquietudes.	Actual	Preventivo	Si	No	Vigente	Líder Tecnología De La Información (Tecnologías de la Información)	
Identificación de proveedores tecnológicos con experiencia en su campo de acción.	01	Para definir un proveedor tecnológico, que en su campo de acción sea bueno para la entidad, es importante definir unas características mínimas de cumplimiento y realizar la comparación antes de iniciar la fase contractual.	Actual	Preventivo	Si	No	Vigente	Líder Tecnología De La Información (Tecnologías de la Información)	Manual
Seguimiento a la ejecución del mantenimiento correctivo de los servicios tecnológicos de la entidad.	02	Mediante el seguimiento a los mantenimientos correctivos se puede determinar si un servicio tecnológico está funcionando correctamente o necesita la intervención del proceso de TI, el proveedor tecnológico o el supervisor del contrato.	Actual	Correctivo	No	Si	Vigente	Líder Tecnología De La Información (Tecnologías de la Información)	Manual
Mantenimiento a las instalaciones y equipos de confort de los centros de cableado, limitando el acceso al personal no autorizado.	01	Los centros de cableado tienen equipos de confort que mantienen en condiciones óptimas estas instalaciones, el objetivo es que esta infraestructura esté funcionando correctamente para que el hardware ubicado no genere fallas.	Actual	Preventivo	Si	No	Vigente	Líder Tecnología De La Información (Tecnologías de la Información)	Manual
Gestión de usuarios, contraseñas y permisos institucionales	01	Debida gestión de usuarios, contraseñas y permisos de personas que tienen acceso a información sensible dentro de la institucional	Actual	Preventivo	Si	No	Vigente	Líder Tecnología De La Información (Tecnologías de la Información)	Manual

Gestión de cláusulas de seguridad y privacidad en los contratos del talento humano que intervengan en la gestión de información institucional y proveedores tecnológicos.	02	En los contratos de los usuarios que administran los sistemas de información y hacen uso de ellos, se deben incorporar cláusulas de privacidad y seguridad de la información.	Actual	Preventivo	Si	No	Vigente	Líder de Contratación (Gestión Contractual y Jurídica), Líder Tecnología De La Información (Tecnologías de la Información)	Manual

C. MONITOREO, SEGUIMIENTO Y REVISIÓN

Teniendo en cuenta los roles y responsabilidades definidos a través de la política de gestión del riesgo, los procesos de: Planeación Institucional, Referente de seguridad del paciente y Tecnologías de la información serán los encargados del monitoreo a los riesgos institucionales, esta actividad se adelantará como mínimo una vez cada cuatrimestre, sin embargo, cada líder de proceso asumirá la responsabilidad de vigilar y retroalimentar cualquier cambio que afecte la concepción de sus riesgos.

El ejercicio de monitoreo de los riesgos por proceso se adelantará a través de la aplicación de una auditoría interna con análisis general de la gestión de riesgos del proceso y análisis particular de cada riesgo identificado por el mismo, donde se evaluará:

- **Análisis general de la gestión del riesgo del proceso:**

1. Consideración de la totalidad de riesgos de acuerdo con los propósitos del proceso evaluado.
2. Reconocimiento de los riesgos identificados y valorados por el proceso.
3. Ejercicio de autocontrol de los riesgos.

- **Análisis particular de cada riesgo:**

Materialización del riesgo: En el análisis de cada riesgo, se indagará la posible presentación de eventos relacionados con el riesgo, las posibles fuentes son: PQRSD, Mesa de ayuda o atención a ciudadanía, oficina jurídica, líneas internas de denuncia, reportes de indicios de atención insegura, ocurrencia de incidentes y/o eventos adversos e indicadores de evaluación.
Atributos del control: Se evaluará si el control se encuentra formalizado a nivel institucional a través de un documento que le normalice, así como su coherencia, pertinencia y eficacia en el tratamiento del riesgo.
Aplicabilidad del control: Se evaluará de manera aleatoria soportes de ejecución del control de acuerdo con su descripción.

SEGUIMIENTO Y EVALUACIÓN
El seguimiento de los riesgos se adelantará únicamente por el proceso de evaluación institucional, oficina de control interno, este se adelantará de manera general como mínimo dos veces en el año.

Para el caso puntual de los riesgos de corrupción:

Seguimiento: El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

- Primer seguimiento: Con corte al 30 de mayo. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para la ciudadanía.

Eficacia de las acciones de mejoramiento en gestión del riesgo: No. De acciones ejecutadas frente a la gestión del riesgo en periodo de tiempo/ Total de acciones propuestas para el periodo de tiempo.

Efectividad de controles definidos en gestión del riesgo: No. De controles calificados satisfactoriamente en efectividad / Total de controles definidos para tratamiento de los riesgos institucionales

PROCESO PARA MODIFICAR EL RIESGO

Como resultado del ejercicio autónomo de vigilancia de los riesgos o del monitoreo realizado a los mismos por los procesos de gestión calidad, planeación institucional y tecnologías de la información se podrán realizar ajustes a los diferentes riesgos, valoración y controles asociados, los cuales se adoptarán a través acta de reunión donde participarán como mínimo: el líder del proceso y el líder de calidad o planeación según aplique.

3. **PLAN DE IMPLEMENTACIÓN**

Teniendo en cuenta el objetivo de la entidad, para disminuir la probabilidad o mitigar el impacto de los riesgos, para la vigencia 2024, de opta por intervenir el riesgo con mayor nivel de riesgo, el cual pertenece a:

Código	Nombre	Probabilidad (Riesgo Inherente)	Impacto (Riesgo Inherente)	Nivel de Riesgo (Riesgo Inherente)
R-TI02	Posibilidad de encriptación o secuestro de la información digital de las bases de datos de los sistemas de información y archivos de los equipos de cómputo.	Media (60%)	Catastrófico (100%)	Extremo

Que genera una actividad correctiva o acción de mejora relacionada a:

Oportunidad de mejora identificada	Tipo de acción a desarrollar	Plan de acción			
	Acción preventiva/ correctiva/ mejora.	Actividad	Responsable	Fecha inicio	Fecha final
Implementar una solución profesional de seguridad perimetral.	Acción correctiva.	Implementar una solución profesional de seguridad perimetral, basada por el cuadrante magico de Gartner, cuya administración sea realizada por una empresa con experiencia en ciberseguridad y se garantice la gestión de politicas de seguridad y correcto funcionamiento de los equipos entregados. Soporte: Informe de implementación de una solución de seguridad perimetral y conexión entre sedes anexas.	Lider de Tecnologías de la Información.	01 Ene. 2025	30 Jun 2025

4. **CAPACITACIÓN**

La socialización del Plan de Tratamiento de Riesgos de Seguridad de la Información, se realizará principalmente en las reuniones directivas, en las cuales, el personal directivo de la entidad, líderes y coordinadores tiene una participación directa con la adopción de las políticas de seguridad de la información y de esta forma, hacerlos participes de los riesgos institucionales en relación a Seguridad Digital.

Los colaboradores, contratistas y terceros, tendrán una ayuda audiovisual para conocer el documento y los riesgos, ya que una buena gestión del conocimiento, permite mitigar la ocasión de incidentes de seguridad. Adicionalmente en los procesos de capacitación institucional, será informado al personal los temas de seguridad y privacidad de la información y riesgos de seguridad Digital.

Bibliografía

Dirección de Gestión y Desempeño Institucional diciembre de 2020. (s.f.). Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública, versión 5.

Ministerio de Tecnologias de la Información y Comunicaciones. (2016). Guia de gestión de Riesgos Seguridad y Privacidad de la Información.

Ministerio de Tecnologias de la Información y Comunicaciones. (OCTUBRE 2021). Documento Maestro del Modelo de Seguridad y Privacidad de la Información. Modelo de Seguridad y Privacidad de la Información.