Centro de Especializaciones Noeder

Diploma de Especialización Internacional

IMPLEMENTADOR Y AUDITOR SEGURIDAD DE LA INFORMACIÓN - ISO 27001 Y CONTINUIDAD DEL NEGOCIO - ISO 22301

MÓDULO II

IMPLEMENTACIÓN DE LA NORMA ISO 27001

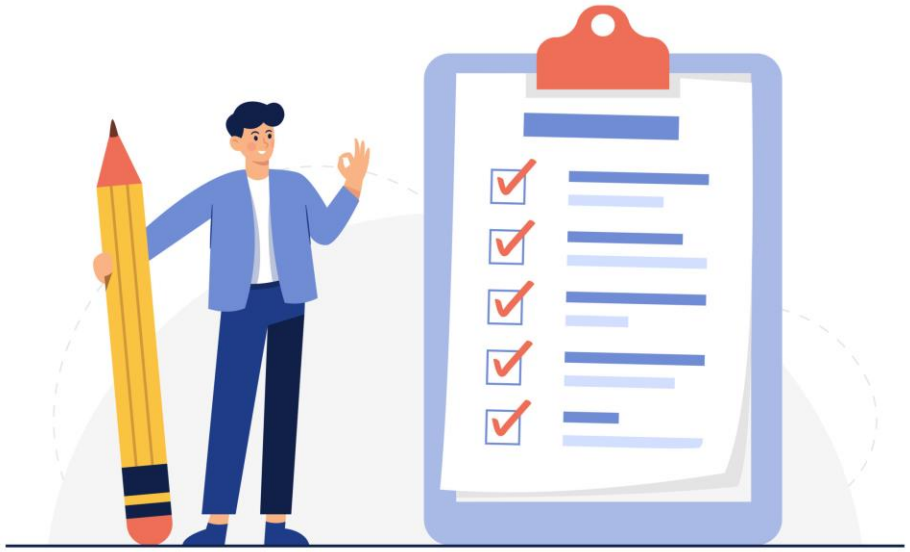
CLASE 04

Mg. Ing. Julio Pereyra Rosales

1. Evaluación de riesgos

8. Operación

8.2 Evaluación de riesgos



La organización debe efectuar evaluaciones de riesgos de seguridad de la información **a intervalos planificados**, y cuando se propongan o se produzcan modificaciones importantes, teniendo en cuenta los criterios establecidos en el punto 6.1.2.

8. Operación

8.2 Evaluación de riesgos

NIVELES DE RIESGO EN EL AMBIENTE DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

8. Operación

8.2 Evaluación de riesgos

Evaluar, Orientar, Supervisar

Ítem	Preguntas
1	¿La Institución cuenta con una unidad específica que administre el entorno tecnológico?
2	En caso que la respuesta del punto 1 sea afirmativa, ¿Depende directamente de la máxima autoridad de la Institución?
3	¿Se cumple con lo establecido en los artículos del Decreto de la Presidencia de la República-Ministerio del Interior N° 6234 del 08/11/16, "Por el cual se declara de interés nacional la aplicación y uso de las Tecnologías de la Información y Comunicación (TIC) en la Gestión Pública, ¿se define la estructura mínima con la que deberá contar y se establecen otras disposiciones para su efectivo funcionamiento"?
4	¿La Institución cumple con lo establecido en el Modelo de Gobernanza de Seguridad de la Información, de acuerdo a lo establecido en la Resolución MITIC N° 733 del 26/12/19?
5	¿La Institución tiene en cuenta la Resolución MITIC N° 277 del 23/06/2020 para establecer los controles sobre la ciberseguridad?
6	¿Se encuentra la administración de TIC alineada a los objetivos de generales de la organización?
7	¿La máxima autoridad apoya el cumplimiento de los planes estratégicos de TI?
8	¿La máxima autoridad conoce la importancia de TIC y su papel con las actividades de la Institución?
9	¿La unidad de TIC comunica sus planes a las partes interesadas de la Institución y dueños de procesos?
10	¿La unidad de TIC comunica sus actividades, retos y riesgos regularmente a la máxima autoridad?
11	¿Se realiza el monitoreo de los avances del plan estratégico y reacciona en consecuencia para cumplir con los objetivos establecidos?
12	¿Se evalúan periódicamente las estructuras, normas y procesos de TIC? Se encuentran operando efectivamente.

8. Operación

8.2 Evaluación de riesgos

Alineación, Planificación y Organización

Ítem	Preguntas
1	¿Se encuentra establecida la estructura de la unidad de TIC acorde a las necesidades de la Institución?
2	¿Están las funciones y responsabilidades de las unidades de TIC definidas, documentadas y entendidas?
3	¿Los encargados de la administración de TIC hacen el seguimiento del cumplimiento de las políticas y procedimientos?
4	¿Los encargados de la administración de TIC tienen conocimientos y experiencia para cumplir con sus responsabilidades?
5	¿El área de TI cuenta con recursos humanos suficientes para apoyar de manera apropiada a las metas, objetivos de la Institución y los procesos de TIC?
6	¿Se encuentran definidos los propietarios de datos y sistemas?
7	¿La propiedad y responsabilidad de los datos fue comunicada a interesados y estos las han aceptado?
8	¿Para la gestión de TIC se ha implementado una adecuada división de roles y responsabilidades para controlar que un mismo individuo no tenga dominio de más de un proceso crítico?
9	¿La Institución ha adoptado y promovido la cultura de gestión de TIC, incluyendo el código de ética y las evaluaciones de los recursos humanos de TIC?
10	¿Se realizan socializaciones y programas de formación continua en TIC que incluyan la conducta ética, las prácticas de seguridad del sistema, las normas de confidencialidad, las normas de integridad y de las responsabilidades de seguridad de todo el personal?
11	¿Se realizó la evaluación de los riesgos referidos a los procesos informáticos y el impacto para el logro de los objetivos institucionales?
12	¿Para la evaluación de riesgos se tuvo comunicación directa y realizaron consultas a las áreas funcionales de la Institución?
13	¿Para la evaluación de riesgos se tuvo en cuenta los factores internos y externos que pueden afectar el logro de los objetivos?
14	¿Para la evaluación de riesgos, se tuvieron en cuenta los contextos: de la organización, de los departamentos, proyectos, ¿las actividades individuales y los riesgos específicos?
+15	¿Se identificaron los principales factores que contribuyen con los riesgos definidos?, por ejemplo: los puntos débiles en los sistemas y en la organización; uso masivo de tecnología; conexión a internet; usuarios poco conscientes de los riesgos etc.

8. Operación

8.2 Evaluación de riesgos

Entrega, servicio y soporte

Ítem	Preguntas
1	¿Se establece y mantiene un plan que permita a TIC responder a incidentes e interrupciones de servicio y la operación continua de los procesos críticos, para mantener la disponibilidad de la información a un nivel aceptable por la Institución?
2	¿Todos los usuarios de sistemas están identificados de manera única y tienen derecho de acceso de acuerdo con sus roles en la Institución?
3	¿Se implementaron medidas lógicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida? Ejemplo: Firewall, Antivirus, actualización de parches de seguridad, otros.
4	¿Se implementaron medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida? Ejemplo: Acceso físico, refrigeración, sistema de extinción, detector de humo, otros.
5	¿Se cuenta con plan de continuidad y contingencias?

Supervisar, Evaluar y Valorar

Ítem	Preguntas
1	¿Se realiza de forma continua evaluación y supervisión, de control interno al área de TIC?
2	¿La gestión de TIC ha establecido métricas apropiadas para gestionar con eficacia las actividades del día a día del departamento de TIC?
3	¿Los responsables de la administración de TIC, monitorean la prestación de servicios para identificar deficiencias y establecen planes de acción concretos de mejoramiento? Ejemplos: rendimiento de la red; estado físico de los equipos; detección de incidentes; calidad de los servicios; definir, documentar, acordar, monitorear, y revisar el desempeño de los servicios prestados.
4	¿Los responsables de la administración de TIC realizan revisiones independientes de sus operaciones? Ejemplos: controles de cambio a sistemas; cumplimiento de objetivos; habilitación de usuarios etc.
5	¿Existe un mecanismo de control interno para permitir el monitoreo de los proveedores de servicios tercerizados?
6	¿Se realizan copias de respaldo de los datos contenidos en las bases de datos?
7	¿Se cuenta con sitio alterno de resguardo de las copias?
8	¿Se realizan pruebas de restauración de las copias?

8. Operación

8.2 Evaluación de riesgos

Áreas de Gobierno	Instituciones	Evaluar, Orientar, Supervisar	Alineación, Planificación y Organización	Entrega, Servicio, Soporte	Supervisar, Evaluar, Valorar	Riesgo por Entidad	Riesgo
Poder Ejecutivo	Procuraduría General de la República	0,50	0,00	0,00	0,12	0,18	BAJO

El nivel de riesgo BAJO, indica que existe una probabilidad mínima de que ocurran eventos no deseados o se presenten impactos negativos en las operaciones de TIC y la entrega de servicios, considerando que fueron aplicados los mecanismos básicos de control planteados en el instrumento del sondeo.

8. Operación

8.2 Evaluación de riesgos

Informe primer cuatrimestre
Riesgos de Seguridad de la información - 2024

Oficina de Tecnologías de la Información y las Comunicaciones

8. Operación

8.2 Evaluación de riesgos

No. de Riesgo	¿QUÉ? IMPACTO	¿CÓMO? CAUSA INMEDIATA	¿PORQUÉ? CAUSA RAÍZ	DESCRIPCIÓN DEL RIESGO	TIPO	SELECCIONE FUENTE GENERADORA DEL EVENTO
R1	Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la informacion de la entidad	Por ausencia de copias de seguridad al momento de presentarse algun evento como daño físico, catastrofes naturales, perdida de los servicios esenciales, fallas técnicas que pone en amenaza la informacion de la entidad.	Debido a inconvenientes y demoras en los procesos contractuales o falta de monitoreo al momento de realizar las copias de seguridad	Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la informacion de la entidad Por ausencia de copias de seguridad al momento de presentarse algun evento como daño físico, catastrofes naturales, perdida de los servicios esenciales, fallas técnicas que pone en amenaza la informacion de la entidad. Debido a inconvenientes y demoras en los procesos contractuales o falta de monitoreo al momento de realizar las copias de seguridad	G Daños Activos Físicos	Evento Externo
R2	Posibilidad de Perdida de disponibilidad e integridad en la infraestructura tecnologica critica de la entidad	Por la ocurrencia de algun evento como daño físico, catastrofes naturales, perdida de los servicios esenciales, fallas técnicas que pone en amenaza la infaestructura tecnologica de la entidad	Debido a inconvenientes y demoras en los procesos de restauracion o falta de dispositivos de respaldo	Posibilidad de Perdida de disponibilidad e integridad en la infraestructura tecnologica critica de la entidad Por la ocurrencia de algun evento como daño físico, catastrofes naturales, perdida de los servicios esenciales, fallas técnicas que pone en amenaza la infaestructura tecnologica de la entidad Debido a inconvenientes y demoras en los procesos de restauracion o falta de dispositivos de respaldo	G Daños Activos Físicos	Evento Externo
R3	Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la infraestructura onpremise e informacion de la entidad	Por la ocurrencia de algun evento de ciberseguridad que ponen en amenaza la infaestructura tecnologica onpremise y la informacion de la entidad	Debido a que un cibercriminal traspasa los controles de seguridad de la entidad	Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la infraestructura onpremise e informacion de la entidad Por la ocurrencia de algun evento de ciberseguridad que ponen en amenaza la infaestructura tecnologica onpremise y la informacion de la entidad Debido a que un cibercriminal traspasa los controles de seguridad de la entidad	G Daños Activos Físicos	Evento Externo
R4	Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la infraestructura web e informacion de la entidad	Por la ocurrencia de algun evento de ciberseguridad que pone en amenaza la infaestructura y aplicaciones web de la entidad	Debido a que un cibercriminal traspasa los controles de seguridad de la entidad	Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la infraestructura web e informacion de la entidad Por la ocurrencia de algun evento de ciberseguridad que pone en amenaza la infaestructura y aplicaciones web de la entidad Debido a que un cibercriminal traspasa los controles de seguridad de la entidad	G Daños Activos Físicos	Evento Externo

8. Operación

8.2 Evaluación de riesgos

Riesgo 1
Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la información de la entidad Por ausencia de copias de seguridad al momento de presentarse algún evento como daño físico, catástrofes naturales, perdida de los servicios esenciales, fallas técnicas que pone en amenaza la información de la entidad. Debido a inconvenientes y demoras en los procesos contractuales o falta de monitoreo al momento de realizar las copias de seguridad.

Controles

1. Líder del proceso de TIC y el Líder de infraestructura verifica Anualmente la continuidad de las licencias y herramientas en las aplicaciones de la entidad. A través de sesiones verifica la necesidad de contratación de herramientas y licencias de las copias de seguridad. En caso de identificar falencias se informa a Líder del proceso de TIC.

Riesgo 2
Posibilidad de Perdida de disponibilidad e integridad en la infraestructura tecnológica critica de la entidad Por la ocurrencia de algún evento como daño físico, catástrofes naturales, perdida de los servicios esenciales, fallas técnicas que pone en amenaza la infraestructura tecnológica de la entidad Debido a inconvenientes y demoras en los procesos de restauración o falta de dispositivos de respaldo.

Controles

1. Líder del proceso de TIC y el Líder de infraestructura verifica semestralmente los planes de mantenimiento de la infraestructura crítica y la restauración, a través de la revisión de los contratos, y validación de las necesidades de mantenimiento de equipos. En caso de identificar falencias se informa a Líder del proceso de TIC.

2. El Líder y equipo de infraestructura monitorea semestralmente el estado de la infraestructura tecnológica. Realizando seguimiento de cada dispositivo critico en la infraestructura de la entidad. En caso de identificar falencias se informa a Líder del proceso de TIC

8. Operación

8.2 Evaluación de riesgos

Riesgo 3
Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la infraestructura onpremise e información de la entidad Por la ocurrencia de algún evento de ciberseguridad que ponen en amenaza la infraestructura tecnológica onpremise y la información de la entidad Debido a que un cibercriminal traspasa los controles de seguridad de la entidad.

Controles

1. El oficial de seguridad de la entidad ejecuta trimestralmente la implementación del MSPI, A través de acciones, tareas, actividades y evidencias de los dominios, en caso de identificar falencias se informa a Líder del proceso de TIC.

2. Líder del proceso de TIC y el Líder de infraestructura verifica semestralmente los contratos con los proveedores y los planes de restauración de los servicios. A través de sesiones verifica la necesidad de contratación de herramientas y licencias de las copias de seguridad. En caso de identificar falencias se informa al comité correspondiente.

Riesgo 4
Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la infraestructura web e información de la entidad Por la ocurrencia de algún evento de ciberseguridad que pone en amenaza la infraestructura y aplicaciones web de la entidad Debido a que un cibercriminal traspasa los controles de seguridad de la entidad.

Controles

1. Líder del proceso de TIC y el Líder de infraestructura verifica trimestralmente garantizando los contratos con los proveedores y los planes de restauración de los servicios, A través de sesiones verifica la necesidad de contratación de herramientas y licencias de las copias de seguridad. En caso de identificar falencias se informa a Líder del proceso de TIC.

2. El oficial de seguridad de la entidad valida trimestralmente estableciendo y ejecutando el plan de análisis de vulnerabilidades web, a través mesas de trabajo y uso de herramientas de especializadas. En caso de identificar falencias se informa a Líder del proceso de TIC.

3. El oficial de seguridad de la entidad realiza trimestralmente realizando el re-testeo de la página y toma las acciones para remediar los hallazgos A través mesas de trabajo y uso de herramientas de vulnerabilidades, remite por correo electrónico los requerimientos y ajustes necesarios En caso de identificar falencias se informa a Líder del proceso de TIC.

8. Operación

8.2 Evaluación de riesgos

5. Materialización de Riesgos.

Durante el primer trimestre de 2024 la Oficina de Tecnologías de la información y las comunicaciones **NO** recibió alertas correspondientes a la posible materialización de riesgos de Seguridad de la información. En las mesas de trabajo realizadas para evaluar los controles y los riesgos actuales, se indagó sobre el tema sin alguna novedad.

2. Tratamiento de los riesgos

8. Operación

8.2 Tratamiento de riesgos.

La organización **debe implementar** el plan de tratamiento de los riesgos de seguridad de la información.

8. Operación

8.2 Evaluación de riesgos

8. Operación

8.2 Evaluación de riesgos

Contenido

III. OBJETIVO

Objetivo General

Detallar el plan de tratamiento de riesgos que hace parte del Sistema de Gestión de Seguridad de la Información – SGSI de la Unidad Nacional para la Gestión del Riesgo de Desastres, mediante el cual se definen los controles que permiten mitigar la materialización de los riesgos de seguridad de la información en la UNGRD.

Objetivos específicos

- ✓ Identificar los riesgos asociados a los procesos y los activos de información que hacen parte del alcance del SGSI.
- ✓ Calcular el nivel de riesgo.
- ✓ Establecer el plan de tratamiento de riesgos.
- ✓ Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos.

8. Operación

8.2 Evaluación de riesgos

IV. ALCANCE

El Plan de tratamiento de riesgos de seguridad de la información es aplicable a todos los procesos de la UNGRD, con alcance a los colaboradores de todos los niveles; desde la identificación de los riesgos de seguridad de la información que se encuentran en los niveles "Alto" y "Extremo" en la Matriz de riesgos de Seguridad de la Información de la UNGRD hasta la definición del plan de tratamiento, responsables y fechas de implementación.

V. METODOLOGÍA

Teniendo en consideración la GUÍA METODOLÓGICA GESTIÓN DE RIESGOS PARA SGSI (G-1101-GTI-01) de la entidad, en la definición del Plan de tratamiento de riesgos de seguridad de la información se realizaron las siguientes actividades en conjunto con los colaboradores asignados para cada proceso de la entidad:

Identificación de los riesgos residuales: Se identifican los riesgos que están en la zona del riesgo residual alto o extremo.

Opción de tratamiento: Campo que se calcula automáticamente de acuerdo con la valoración del riesgo residual, según la zona donde se ubica el riesgo residual, se determina la opción o estrategia de tratamiento a seguir para combatir el riesgo, para esta actividad se debe considerar la siguiente tabla:

ZONA DE RIESGO RESIDUAL	NIVEL DE RIESGO ACEPTABLE	OPCIÓN O ESTRATEGIA DE TRATAMIENTO A SEGUIR
Bajo	Aceptable	Asumir/Aceptar
Moderado	Aceptable	Asumir/Aceptar
Alto	No Aceptable	Reducir/Mitigar
Extremo	No Aceptable	Reducir/Mitigar

Resultado valoración de Riesgos de Seguridad de la Información

La identificación y valoración de riesgos sobre los activos de información de la entidad se encuentra detallada en la Matriz de Gestión de Riesgos de Seguridad de la Información (RG-1101-GTI-04).

A continuación, se discriminan los riesgos de seguridad de la información identificados por nivel de riesgo residual:

Nivel del Riesgo	Cantidad de Riesgos	Porcentaje%
Bajo	25	64.1%
Moderado	11	28.2%
Alto	1	2.6%
Extremo	2	5,1%
TOTAL	39	100%

Si el riesgo se ubica en una zona no aceptable, cada líder responsable de los riesgos identificados con el apoyo del Grupo de Tecnologías de la Información, debe definir e implementar los controles necesarios para llevar el riesgo a un nivel aceptable a través del plan de tratamiento de riesgos. Se establecieron las siguientes acciones de mejora para abordar los tres (3) riesgos en valoraciones alta y extrema:

8. Operación

8.2 Evaluación de riesgos

IDENTIFICACION DEL RIESGO					ZONA DE RIESGO RESIDUAL	PLAN DE TRATAMIENTO					
ID	PROCESO	TIPO DE ACTIVO DE INFORMACIÓN	RIESGO	DESCRIPCIÓN DEL RIESGO		OPCIÓN DE TRATAMIENTO	ACCIONES DE MEJORA	CONTROL ANEXO A NTC-ISO-IEC 27001:2013	SOPORTE	RESPONSABLE	Fecha implementación
18	Gestión de tecnologías de la información	Hardware	Confidencialidad	Afectación reputacional y legal por ataque informático debido a desconocimiento de las políticas para el buen uso de los activos de información (Red, Correo, Internet, Sistemas de Información, Chat, Redes Sociales, etc.) por parte de los colaboradores.	**Extremo**	Reducir/Mitigar	Realizar un ejercicio de ingeniería social para todos los colaboradores de la Entidad.	A.7.2.2-Toma de conciencia, educación y formación en la seguridad de la información	Informe del ejercicio	Líder del proceso y proveedor	Primer semestre
31	Servicio al ciudadano	Software	Confidencialidad	Posibilidad de abuso de privilegios debido a asignación errada de los mismos.	**Alto**	Reducir/Mitigar	Solicitar periódicamente al Grupo de Tecnologías de la información mantenimiento y/o actualización del Sistema PQRSD, revisando que los usuarios sean los correctos.	A.9.2.5-Revisión de los derechos de acceso de usuarios	Informe de revisiones	Grupo de tecnología de la información y el Líder del proceso de Servicio al ciudadano	A demanda
37	Gestión de Control Disciplinario	Recurso Humano	Disponibilidad	Ausencia de personal de planta o contratistas conlleva a que no se cumplan con los objetivos del proceso de control disciplinario	**Extremo**	Reducir/Mitigar	Solicitar la contratación de un abogado con experiencia en derecho disciplinario o afines	A.9.2.5-Revisión de los derechos de acceso de usuarios	Documentos precontractuales correspondientes	Líder del proceso	Primer cuatrimestre

8. Operación

8.2 Tratamiento de riesgos.

PLAN DE TRATAMIENTO DE GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8. Operación

8.2 Tratamiento de riesgos.

El Plan de Tratamiento de Riesgos de Seguridad de la Información 2023 contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información del MinTIC.

CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN				Enero				Febrero				Marzo				Abril				Mayo				Junio				Julio				Agosto				Septiembre				Octubre				Noviembre				Diciembre			
Componente	Responsable	Actividad	Tareas	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
Gestión de Riesgos de Seguridad de la Información	Subdirección de Informática y Sistemas	Presentación del Plana Comité de Gestión y Desempeño	Presentar el plan ante el comité																																												
		Sensibilización	Socialización de lineamientos y Herramienta - Gestión de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital.																																												
		Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información.																																												
			Realimentación, revisión y verificación de los riesgos identificados (Ajustes)																																												
		Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento																																												
		Publicación	Publicación mapas de riesgos en las páginas institucionales																																												
		Seguimiento Fase de Tratamiento	Seguimiento a controles y planes de tratamiento de riesgos identificados (verificación de evidencias)																																												

8. Operación

8.2 Tratamiento de riesgos.

VERSIÓN 4.0

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8. Operación

8.2 Tratamiento de riesgos.

Estrategia	Actividades	Evidencia
Revisión/actualización de documentación	Actualizar manual de gestión de riesgos de seguridad digital.	Documento: Manual De Gestión De Riesgos De Seguridad De La Información TIC-MA-007 publicado y aprobado
Concienciación sobre conceptos y bases para la identificación de riesgos	Elaborar piezas gráficas y charlas relacionadas con el mapa riesgos.	Piezas gráficas, listados de asistencia, grabación de charlas y correo electrónico con envío masivo.
Identificación de riesgos de seguridad de la información	Realizar revisión, identificación, gestión y actualización sobre los riesgos de seguridad de la información.	Mapa de Riesgos Actualizado y publicado.

8. Operación

8.2 Tratamiento de riesgos.

Estrategia	Actividades	Evidencia
Plan de tratamiento de riesgos de seguridad de la información	Documentar las actividades relacionadas para implementar los controles establecidos.	Evidencias de los controles, seguimiento y monitoreo de los riesgos.
Aceptación del riesgo de seguridad de la información	Revisar periódicamente de las aprobaciones de las matrices de riesgos de seguridad por el propietario del riesgo (líder del proceso) como declaración formal de la aceptación.	Correo electrónico/memorando
Seguimiento planes de tratamiento de riesgos de seguridad de la información	Revisar la documentación y evidencias de los seguimientos realizados al plan de tratamiento.	Correo electrónico, Actas de sesiones
Mejoramiento	Identificar oportunidades de mejora conforme los resultados de la evaluación del riesgo residual.	Correo electrónico, Actas de sesiones
Monitoreo	Reportar actividades de seguimiento a través del plan e indicadores.	Publicación de informes de seguimiento a los riesgos de manera cuatrimestral.

¡Gracias!

Centro de
Especializaciones
Noeder

Conócenos más haciendo clic en cada botón