ALCALDÍA DE
SANTIAGO DE CALI

Proceso de contratación: CIBER SEGURIDAD

Objeto: Proporcionar herramientas para soluciones de Seguridad Digital, Seguridad de la Información y Ciberseguridad que proteja la infraestructura tecnológica de la Alcaldía Distrital de Santiago de Cali contra amenazas, riesgos y ciberataques.

Plazo de ejecución: Hasta el 31 de diciembre de 2024.

CONTRATOS	% A APLICAR	DISCRIMINADOS ASÍ:	
Mayores de: $191.648.680 (4,072 UVT)	12,00%	- Pro Desarrollo	3,50%
		- Pro Univalle	2,00%
		- Pro Hospital	1,00%
		- Pro UniPacifico	0,50%
		- Pro Cultura	1,00%
		- Pro Adulto Mayor	2,00%
		- Pro Deporte y Recreación	2,00%

NOTA: De igual manera se debe contemplar la nueva estampilla que entro en vigencia en el mes de agosto de 2024, llamada Pro justicia Familiar 2%, que será aplicada a contratos mensuales por valor => 10 SMMLV (Igual o mayor a $13.000.000).

DESCRIPCIÓN DE LAS ACTIVIDADES A DESARROLLAR

1 Diagnóstico y Planificación

Realizar un análisis del estado actual del SGSI, para lo cual se revisa la política y el alcance del SGSI, se establecen los responsables y las responsabilidades en cuanto a seguridad de la información y se realiza el levantamiento y valoración de activos de información, análisis de vulnerabilidades e identificación de riesgos de seguridad de la información. Además de:

- Actualizar el nivel de madurez en seguridad de la información con relación a la Norma ISO/IEC 27001:2022
- Identificar el estado actual de la Gestión de Seguridad de la Información de acuerdo a lo contemplado en el Mapa de Procesos que cuenta la entidad.
- Realizar la identificación, valoración y clasificación de los activos de información que posee la entidad.
- Análisis de vulnerabilidades: Identificar las amenazas y vulnerabilidades a las que se encuentra expuesta la Entidad tanto en servidores, equipos de cómputo, activos de red, sistemas de información esto para un máximo de 500 activos.

- Gestión de Riesgos de Seguridad de la Información para los procesos incluidos. Adoptar y ajustar, la metodología de gestión del riesgo. Que incluye, análisis, evaluación y mitigación del riesgo, basados en la Norma ISO 27005:2013 o Norma ISO 31000.

El diagnóstico de seguridad incluye:

- Realizar entrevistas con las diferentes áreas para levantar el inventario de activos de información, entiéndase como activo de información de acuerdo a la definición de la ISO 27000:2022 (En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización).
- Revisar las Políticas de Tecnología de Información, esquemas de copias de seguridad o respaldo y esquemas de impresión.
- Identificar la topología física y lógica de la red.
- Revisar la documentación existente.
- Evaluar y desarrollar las políticas de seguridad de la información que requiera la entidad.
- Formular una propuesta que permita dar tratamiento de Políticas de Seguridad en la entidad que contempla:
    - Definición de los procedimientos para el manejo de la documentación.
    - Control de cambios.
    - Definición de roles y responsabilidades del personal involucrado en el mantenimiento de las políticas de seguridad de la información.
    - Gestión de incidentes.

Para la valoración y clasificación de los activos de información identificados se desarrollan las siguientes actividades:

- Evaluación de los procesos, procedimientos y actos administrativos existentes en la Entidad relacionada con el tema de seguridad de la información.
- Evaluación del estado actual de los sistemas de información en cuanto a su seguridad, teniendo en cuenta los siguientes aspectos:
- Procedimientos de control cambios.
- Procedimientos de administración del sistema.
- Esquemas de acceso al sistema de información.
- Niveles de integridad, confidencialidad y disponibilidad en cuanto a acceso permitido.
- Almacenamiento y archivado, disposición y destrucción.
- Administración y controles existentes sobre las bases de datos
- Procedimientos de respaldo de información.

En la identificación de las amenazas y vulnerabilidades a las que se encuentra expuesta la Entidad ejecutan pruebas de vulnerabilidad en un máximo de **500 activos**.

El análisis de vulnerabilidades implica desarrollar las siguientes actividades:

- Análisis de vulnerabilidades para determinar las debilidades existentes de los servicios a nivel interno y externo, aplicando las recomendaciones del OSSTMM.
- Realizar la delimitación del perímetro y verificación de la red de la entidad.
- Evaluar la configuración de los firewalls, entre otros: lista de acceso, análisis de los puertos, los servicios abiertos, entre otros.
- Realizar prueba de intrusión en la red de área local (LAN) tanto alámbrica como inalámbrica y con base en esta determinar el estado actual de la infraestructura tecnológica.
- Realizar prueba de penetración a 10 IPs públicas, con el fin de determinar el estado actual de la infraestructura tecnológica y la seguridad de su interconexión.
- Realizar análisis de vulnerabilidades en los hosts.

1.1 Pruebas de Ingeniería Social

Ejecución de Ingeniería social presenciales (en las instalaciones de la Entidad) y no presenciales.

- **Pruebas presenciales**

Análisis del nivel de cumplimiento y madurez de los siguientes controles especificados en el dominio N.º 11 de la norma ISO 27001:2022 (seguridad física y ambiental) como son:

  - Áreas de acceso público
  - Seguridad de los equipos
  - Emplazamiento y protección de equipos
  - Instalaciones de suministros
  - Seguridad de los equipos y activos fuera de las instalaciones
  - Revisión del cumplimiento de la política de escritorio limpio y pantalla bloqueada, determinando los horarios habituales en que los colaboradores no se encuentran en su sitio de trabajo y ejecutando revisiones presenciales para constatar el cumplimiento de los aspectos que comprenden el diagnóstico.

- Pruebas no presenciales

Estarán orientadas a la utilización de medios informáticos como el correo electrónico, redes sociales e internet y se realizarán con recursos propios del contratista, de los mecanismos a utilizar y los tiempos en los que se ejecutarán.

Las pruebas contemplan:

- Recolección de información que vincule a la entidad, en internet y redes sociales.
- Haciendo uso de técnicas como Google hacking, búsqueda de metadatos y cualquier otra que el contratista proponga y sea aprobada previamente por la entidad, se realiza recolección de información que vincule a la entidad, en Internet y redes sociales, realizando búsqueda de archivos, usuarios y claves de correo o de dominio, nombre de impresoras, maquinas, software, sistemas operativos, extensiones telefónicas, datos personales de los funcionarios de la entidad, entre otra información que se considere relevante. Esto, con el propósito de establecer si es posible encontrar información privilegiada de la entidad y/o sus funcionarios publicada en la red, que pueda ser aprovechada por terceros generando exposición a riesgos de seguridad de la información.

Fake Mailing

Envío de correos electrónicos haciendo uso de la técnica mail relay, a través de un servidor de correo que lo permita a cuentas de correo de la entidad, previamente definidos por la entidad, para lograr los siguientes objetivos:

- Intentar obtener información privilegiada
- Intentar obtener nombres de usuarios y/o contraseñas
- Intentar que el usuario responda y/o reenvíe el correo

Suplantación de un servicio web o intento de phishing

Intento o materialización de un ataque de phishing por medio del correo electrónico con el cual se intente que los receptores del mensaje ingresen a un link y accedan a una página web con las mismas características de algún servicio web provisto por la entidad.

Gestión de Riesgos de Seguridad de la Información.

Para adoptar y ajustar la metodología de gestión de riesgos de seguridad de la información, basado en la Norma ISO 27005 o Norma ISO 31000 la ISO 27005, ISO 31000 se ejecutan las siguientes actividades:

- Revisar la metodología de gestión de riesgos y adoptarlo al SGSI para identificar los riesgos de seguridad de la información, de acuerdo a la norma ISO 27001:2022.
- Si la entidad a la fecha cuenta con matriz de riesgos de los activos de información se revalida y actualiza, de lo contrario se construye con el acompañamiento de los dueños de los procesos, la cual contendrá los requerimientos mínimos de gestión del riesgo de la norma ISO/IEC 27001:2022

Entregables

Como resultado del monitoreo e identificación de las posibles vulnerabilidades, se deben entregar los siguientes productos:

- Informe con la identificación del nivel de madurez resultado del análisis GAP.
- Inventario de activos de información de los procesos del alcance
- Documento con la propuesta de instructivo de clasificación y etiquetado de activos de información.
- Documento que contenga la propuesta de política, el alcance y los objetivos del SGSI.
- Documento que contenga la propuesta de los procesos y procedimientos necesarios para el mantenimiento del esquema de políticas de seguridad de la información.
- Informe del análisis de vulnerabilidades.
- Informe de los resultados de pruebas presenciales y no presenciales.
- Gestión de riesgos de seguridad de la información: Documento con la metodología de la gestión de riesgos.
- Matriz de valoración riesgos de seguridad de la información
- Documento con el plan de tratamiento de riesgos

2 Implementación

Corresponde a la ejecución de todo lo planeado con el fin de monitorear resultados y efectuar acciones de retroalimentación y así la implementación del plan de tratamiento de riesgos, implementación de controles e implementación del Subsistema de Gestión de Seguridad de la Información (SGSI), definir el plan de continuidad de negocio (BCP) con su respectivo Análisis de impacto al negocio (BIA).

Así mismo, se pretende medir el estado actual frente al cumplimiento de cada requisito de la norma, es decir, se verifica si se ha ejecutado lo planeado. Se incluye la medición del SGSI, requisitos legales, del cliente y de la organización

Además de:

- Implementación del SGSI a los procesos de la entidad de acuerdo al alcance establecido
- Definir Plan de contingencia y de continuidad del negocio (BCP)
- Definir Análisis de impacto al negocio (BIA)
- Implementar los procedimientos del SGSI
- Evaluar el cumplimiento de las políticas/procedimientos implementados

2.1 Actividades a Desarrollar

- Crear, revisar y/o actualizar el Plan de contingencia y de continuidad del negocio (BCP), Análisis de impacto al negocio (BIA) y el Plan de recuperación de Desastres (DRP) con que cuenta la Alcaldía acorde con las necesidades de Alcaldía de Santiago de Cali
- Definir los indicadores adecuados para la medición del SGSI.
- Revisar la eficiencia, efectividad y eficacia del SGSI
- Revisión del tipo de información que genera la entidad y su esquematización frente a la Ley de transparencia. Análisis de los lineamientos expedido por MinTic para publicación de la información pública.
- Establecimiento de los lineamientos y condiciones sobre medios para recepción de solicitudes de información pública. Análisis de requisitos a formular para la atención ciudadana y condiciones de seguridad de la información.
- Análisis sobre información clasificada y reservada. Índice de información clasificada y reservada. Protocolo de etiquetado y clasificación de información.

Entregables

➢ Plan de tratamiento de riesgos

➢ Informe de la ejecución del plan de tratamiento de riesgos.

➢ Documento con la declaración de aplicabilidad.

➢ Evidencias de las actividades de implementación de procedimientos del SGSI

➢ Definición Del Modelo De Seguridad SGSI

Documento con el modelo de seguridad que contiene:

➢ Política del SGSI

➢ El alcance del SGSI

➢ Objetivos del SGSI

➢ Manual de políticas de seguridad de la información

➢ Documento con la definición de los roles y responsabilidades en la SGSI

➢ Documento con el Plan de continuidad del negocio (BCP)

➢ Documento con el Análisis de impacto al negocio (BIA)

Seguimiento SGSI

➢ Documento que contenga lo indicadores propuestos para el SGSI

➢ Valoración de los indicadores del SGSI.

3 Sensibilización y Capacitación

Diseñar una campaña y estrategia de sensibilización y divulgación de políticas y procedimientos de SGSI. Así como Evaluar el cumplimiento de las políticas/procedimientos implementados.

3.1 Actividades a Desarrollar

Se proponen 5 actividades de sensibilización y divulgación en cultura de seguridad para los funcionarios de la Alcaldía de Santiago de Cali, las cuales se definen de manera independiente; para validación y selección de las que la entidad considere deben ser ejecutadas por parte del contratista en el proyecto.

Las propuestas deben contemplar las siguientes alternativas:

a) 1 Performance de lanzamiento – representación teatral en la Entidad, Organismos ubicados en el CAM, debe de estar compuesto por mínimo 3 personas, 120 elementos de suvenir.

b) 2 Talleres de sensibilización en temas de seguridad de mínimo 2 horas cada uno al grupo CTO. 120 elementos de suvenir.

c) 2 Conferencias en temas de seguridad con ayudas audiovisuales a las partes interesadas.

La planeación y coordinación de la logística para la realización de la sensibilización y divulgación de temas de seguridad deben ser acordadas las propuestas seleccionadas por la Entidad.

Elaboración del material para la divulgación y sensibilización a los funcionarios de la Entidad, incluye 2 videos, 2 wallpapers, 1 pendón, souvenirs. Validados con la entidad.

Ejecución de la sensibilización y divulgación en temas de seguridad de acuerdo con las propuestas aprobadas por la Entidad.

Entregables

- Documento con el plan de sensibilización y divulgación de seguridad.
- Documento que contiene el plan de ejecución de la sensibilización y divulgación de seguridad.
- Documento que contiene el plan de promoción de sensibilización y divulgación de seguridad.
- Material de promoción para realizar la sensibilización y divulgación en temas de seguridad. • Evidencias de las actividades de sensibilización

4. Suministro de herramienta de software para la gestión del SGSI

Como apoyo para la prestación del servicio, se debe suministrar un servicio web especializado en la administración y gestión del SGSI POR 2 AÑOS el cual es una herramienta que ayuda a las organizaciones en la implementación, gestión y mantenimiento de Sistemas de Gestión.

Este debe contar con acceso para 4 administradores, 20 usuarios e ilimitados registros de Activos de información. Este debe de cumplir de manera efectiva con la normativa vigente en materia de implementación de SGSI (ISO/ICE 27001:2022). Todos los módulos complementarios e integrados que posee el software deberán ayudar con el cumplimiento legal y regulatorio a toda la organización.

La herramienta debe ser totalmente funcional en un ambiente web que facilita la labor entre todos los integrantes y responsables de su SGSI que puede ser utilizado en cualquier dispositivo.

El cumplimiento de la norma requiere la realización de determinadas tareas por parte de los encargados del SGSI al interior de la entidad; El software debe contar con módulos que automatizan dichas actividades.

MODULOS

El Software debe tener una vigencia de 24 Meses desde el contrato inicial, esta herramienta debe tener las siguientes generalidades.

- Debe poder establecer controles de ingreso por usuario, con asignación de roles y grupos de usuarios
- Facilitar el cargue de tablas básicas pre diligenciadas como procesos, activos, riesgos y en general los datos que la entidad requiera para parametrizar adecuadamente la aplicación.
- Permitir la fácil consulta a través de filtros con combinación de criterios que permitan obtener reportes en los diferentes módulos del sistema de información.
- Poder controlar y hacer auditoria para identificar la trazabilidad de los

registros y acciones de los usuarios tales como accesos, creación de registros, eliminación, modificación.
- Se integra al correo electrónico para él envió de notificaciones.
- Contar con la autenticación de usuarios a través de una integración con el directorio activo.
- Se podrá solicitar una prueba de concepto de la operación del sistema en la etapa precontractual.

Adicional debe contar con módulos para:

GESTIÓN DOCUMENTAL

- Debe Permitir el control de la documentación del SGSI para poder publicar en el mismo las políticas, normas, procedimientos, instructivos, entre otros
- Los documentos se deberán de catalogar según su clasificación y sobre ellos garantizar permisos de consulta por grupos de usuarios.
- Deberá Permitir crear y visualizar la caracterización del proceso de seguridad de la información de manera simple y dinámica.
- Deberá Poder publicar un glosario de términos que permita el uso adecuado del lenguaje y terminología propia del Sistema de Gestión de Seguridad de la Información

GESTIÓN DE RIESGOS

- Deberá de estar en la capacidad de realizar la gestión de riesgos: identificación, tipificación, análisis, tratamiento entre otros.
- En la identificación de Riesgos deberá permitir enlazar los activos de información.
- Debe Permitir la parametrización de probabilidad e impacto, niveles de valoración de riesgos, amenazas, vulnerabilidades por tipos de activos, definición de niveles de riesgo, listado de riesgos, Catálogo de controles y mapa de calor configurables.
- Debe Permitir la comparación de los mapas antes y después de valoración de riesgos y la calificación.
- Debe Establecer cuáles recursos del negocio van a ser considerados dentro del cálculo del impacto del riesgo, (Recurso Financiero, operación, imagen, legal, ambiental, Humano)
- Debe Contar con un catálogo predefinido de amenazas y vulnerabilidades.
- deberá Carga y administrar las causas, factores y consecuencias de los riesgos.
- Permitir Definir la parametrización para los niveles de riesgo residual.
- Debe Permitir generar un plan de tratamiento de riesgos.
- Debe Permitir asociar controles para la gestión de riesgo.
- Debe Permitir la parametrización de la declaración de aplicabilidad.

GESTIÓN DE EVENTOS E INCIDENTES

- Debe Permitir registrar eventos e incidentes de seguridad, asignándole un identificador o ID de manera automática, las actividades realizadas para diagnosticar, analizar, contener el incidente.
- Debe Permitir asignar responsable(s) del incidente, tipificarlo y establecer su impacto, criticidad y tiempos de respuesta.
- Permite escalamiento y notificaciones enlazado con el correo electrónico.
- Debe Permitir consultar las lecciones aprendidas.
- Debe Permitir que cualquier usuario pueda reportar un evento de seguridad de la información.
- Deberá de Contar con reportes gráficos de Top de riesgos con mayores activos, Top de vulnerabilidades con mayores riesgos, Top de amenazas con mayores riesgos, Top de factores con mayores Riesgos, Top de riesgos por procesos
- Deberá de Permitir la definición de diferentes tipos de incidentes.

GESTION DE USUARIOS ROLES Y GRUPOS

- Deberá Brinda a las entidades y organizaciones, la posibilidad de gestionar los usuarios, grupos y roles de forma intuitiva y sencilla, posibilitando la auditoria a usuario, informes de permisos asignados, registro de usuarios por medio de CMS, LDAP (directorio activo), Google o Microsoft, entre otras funcionalidades.

AUDITORIA Y SEGUIMIENTO

- Deberá de Permitir administrar y gestionar de manera integral todo el proceso de auditorías internas de seguridad de la información.
- Deberá de Permitir la creación automática del informe por cada auditoría realizada.
- Deberá de Contar con una opción para revisión por la dirección.
- Deberá de Permitir registrar las correcciones inmediatas a las no conformidades detectadas y acciones de mejora

INDICADORES

- El sistema deberá permitir diseñar y publicar cualquier indicador requerido para el sistema de gestión de seguridad de la información y su respectiva ficha técnica para su respectiva medición, seguimiento y control.
- Deberá Permitir la valoración de indicadores para calificar el cumplimiento de estos con base en variables automáticas que traiga el mismo sistema relacionados como mínimo con la gestión de eventos o incidentes
- Deberá de Genera reportes, gráficos y poseer elementos que permitan hacer un mejor seguimiento, análisis y mejora a la Entidad.

- Deberá Permitir establecer rangos superiores e inferiores y periodicidad de medición

PLAN DE CONTINUIDAD

- Deberá de Permitir registrar las variables críticas del BIA, RTO, RPO.
- Deberá de Registrar los periodos críticos de operación y llevar un registro de interrupciones ocurridas

GESTION DE ACTIVOS

- Deberá de estar en la capacidad de realizar la gestión de activos: identificación, registro, clasificación, criticidad y valoración entre otras
- Debe de Permitir la creación de nuevos campos personalizados para el formulario de creación de activos de información.
- Debe de Permitir el cargue masivo de información previa, mínimo en formato Excel.
- Debe de Contar con un inventario de activos de información que se consulte desde la herramienta y sea exportable.
- Debe de Generar reportes, gráficos y poseer elementos que permitan llevar control de la gestión de activos de información.
- Debe de Permitir la personalización de campos como responsable de activo y custodio.
- Debe de Permitir la valoración de activos según las propiedades de criticidad, disponibilidad e integridad.
-

GESTIÓN DE PROCESOS, OBJETIVOS Y REQUISITOS

- Debe de Permitir el registro de procesos, áreas, cargos y objetivos estratégicos de la entidad u organización, así como la relación de documentos y requisitos legales a los procesos para la gestión de auditorías dentro del módulo de Seguimiento.

GESTIÓN DE TAREAS

- Debe de Contar con un tablero de tareas en donde los usuarios identifiquen las actividades pendientes del sistema de gestión de seguridad de la información.
- Debe de Permitir la configuración de tiempos de gestión de dichas tareas.
- Deberá de Administrar la asignación de tareas para gestionar las actividades propias al sistema.
- Debe de Permitir anexar archivos de evidencia.

ANÁLISIS DE BRECHAS

- Debe de Permitir adicionar y administrar las normas, estándares o leyes sobre las cuales se quiere medir el cumplimiento normativo de seguridad de la información por ejemplo MSPI e ISO 27001.
- Deberá permitir Calificar el nivel de cumplimiento de un control o requisito, navegando por objetivo de control o área de cumplimiento y sub-área o domino.
- Debe de Permitir que los usuarios justifiquen la calificación de cumplimiento con observaciones y recomendaciones.

PROTECCIÓN DE DATOS PERSONALES

- Debe de Permitir el registro y actualización de bases de datos, que se vinculen a encargados, canales, finalidades.
- Debe de Permitir la creación de Encargados para la base de datos.
- Debe de Permitir gestionar los requisitos de la ley de protección de datos

GESTIÓN DE CAMBIOS

- Debe de Permitir a cualquier usuario registrar solicitudes de cambio con el potencial de causar un impacto mayor en los servicios, infraestructura tecnológica o aspectos relacionados con la seguridad de la información.
- Debe de Permitir parametrizar y administrar la gestión de las solicitudes, debe contar con el sistema de notificación vía correo electrónico a través del cual se informa el estado de la solicitud.

Se deberá de realizar Capacitación presencial en el uso de la herramienta a los administradores del sistema de gestión que la organización determine (máximo 4).

Se deberá de tener acceso a las a actualizaciones nuevas versiones de la herramienta.

Se deberá de tener una Mesa de ayuda para soporte de herramienta de lunes a viernes entre las 8 am a 6 pm en días hábiles durante la vigencia de la oferta de la Herramienta, Los canales de atención deberán de ser.

- E-mail
- Chat en Línea
- Telefónico
- Help Desk

ENTREGABLES HERRAMIENTA.

- Suministro del portal web para uso de la herramienta por parte de la Organización.
- Documentación guía y manuales de usuario disponibles en formato electrónico.
- Credenciales de acceso para (4) usuarios administradores de la solución.
- Creación de 20 usuarios iniciales para el uso de la herramienta.

5. CENTRO DE OPERACIÓN DE SEGURIDAD-CORRELACION DE EVENTOS

Prestar el servicio de un Centro de operaciones de Seguridad (SOC) donde se registra y se analiza los logs de eventos de la infraestructura de seguridad de la entidad para determinar si se están presentado eventos que correspondan a posibles ataques cibernéticos o a incumplimientos de políticas de seguridad que pongan en riesgo las operaciones del negocio.

El servicio de SOC se prestará durante el periodo contratado.

Propósito:

Proveer capacidades de monitoreo centralizado y especializado para identificar, detectar y responder adecuada y oportunamente ante los incidentes de seguridad que puedan afectar la información de una organización.

Detectar en el menor tiempo posible los ataques para limitar el daño. La rentabilidad que da un SOC se refleja en el ahorro de dinero que implica tratar rápidamente los incidentes de seguridad.

Se requiere se pueda obtener los beneficios de un servicio de inteligencia, gestionado y controlado y que adicionalmente no tengan que invertir en aspectos o funciones que no son relevantes dentro de las necesidades de apoyo para la gestión de la ciberseguridad.

INFRAESTRUCTURA A MONITOREAR

LINEA BASE DEL SERVICIO

Nodos a Monitorear	Cantidad
Server	200
Workstation	
Network Devices	

ALCALDÍA DE
SANTIAGO DE CALI

ALCANCE SOC

Las actividades generales a realizar en este servicio en modalidad 7x24 incluyen:

- El SOC deberá estar ubicado físicamente en la ciudad de Cali para prestar servicios presenciales en caso de la materialización de un incidente (se podrá validar mediante una visita)
- Monitoreo en la notificación de los eventos u ofensas de seguridad, información sobre amenazas emergentes.
- Detección temprana de ataques a través de analítica de logs generadas desde diferentes fuentes.
- El servicio de SOC deberá estar certificado en buenas prácticas de seguridad mediante la norma ISO27001:2022 y pertenecer al First.org
- Identificar y reportar comportamientos anómalos, no autorizados, fraudulentos y/o sospechosos que atenten contra la disponibilidad e integridad de la información y sistemas correlacionados.
- Entrega mensual de un informe durante la vigencia del contrato que incluye: Top de Reportes, eventos, recomendaciones, lecciones aprendidas, informe de vulnerabilidades.
- Alcance en configuración de reglas simples y de correlación
- Configuración de Dashboard Básicos

CORRELACION DE EVENTOS

La Gestión de Eventos se puede definir como el proceso que se encarga detectar cambios significativos para tomar las medidas de control necesarias según determinen estos eventos. Esto quiere decir que la Gestión de Eventos es la base para la supervisión y el control de las operaciones de Seguridad y de TI.

El proceso de gestión de eventos contempla las siguientes actividades:

TAREA	DESCRIPCION
Mantenimiento de Mecanismos y Reglas de Monitorización de Eventos	Establecer y mantener los mecanismos para generar reglas efectivas para los procesos de descarte y correlación de Eventos.
Clasificación y Categorización de Eventos	Clasificar aquellos eventos que se pueden obviar, y asignar categorías a los que son significativos.
Correlación de Eventos y Selección de Respuestas	Interpretar el significado de un Evento y elegir una respuesta adecuada.
Revisión y Apoyo Cierre de Eventos	Verificar que los Eventos hayan sido manejados adecuadamente y si se pueden cerrar. Este proceso también sirve para asegurar que los registros de eventos sean analizados de manera que se identifiquen tendencias y patrones que puedan sugerir medidas correctivas necesarias.

Las actividades generales a realizar en este servicio incluyen:

- Gestión y correlación de eventos.
- Monitoreo, gestión en la notificación de los eventos u ofensas de seguridad, información sobre amenazas emergentes.
- Apoyo a la Atención de incidentes y apoyo a la investigación de causa raíz sobre los eventos de seguridad que se materialicen
- Detección temprana de ataques a través de analítica de logs generadas desde diferentes fuentes de Alcaldía de Santiago de Cali.
- Identificar y reportar comportamientos anómalos, no autorizados, fraudulentos y/o sospechosos que atenten contra la disponibilidad e integridad de la información y sistemas correlacionados.
- Entrega mensual de un informe durante la vigencia del contrato, el cual incluya los incidentes detectados, así como las acciones de prevención, detección y respuesta frente a eventos de seguridad identificados.

Descripción de los servicios del SOC

El SOC prestara de manera remota la atención de primer nivel de los incidentes detectados, escalando al grupo de seguridad de Alcaldía de Santiago de Cali.

Los eventos de prioridad crítica y alta serán notificados al grupo de seguridad del ALCALDIA a través del contacto telefónico provisto para tal fin. Los eventos de prioridad media, baja e informativos también serán notificados vía correo electrónico.

Operación:

- Monitoreo de la plataforma tecnológica de monitoreo.
- Gestión de requerimientos básicos de plataforma bajo los esquemas ya establecidos para estos casos.
- Apoyo especializado a la Gestión con los ingenieros expertos de Alcaldía de Santiago de Cali en caso de presentarse alguna incidencia que afecte la operación de esta.
- Gestión de todos los incidentes requerimiento (entre nivel uno).

ACUERDOS DE NIVELES DE SERVICIO

	NIVEL DE CRITICIDAD		
	Alta	Media	Baja
Gestión de eventos (7x24) *Notificación de Alarma	2 horas	4 a 6 Horas	8 a 24 Horas

- Todas las alertas con criticidad "Baja" serán reportadas en el informe mensual de servicio; si estas son reiterativas durante un periodo de tiempo especificado, serán reportadas al cliente en el tiempo mencionado en el cuadro.
- Se utilizará 30 Minutos para reportar el incidente.

SERVICIOS DE GESTION DE INCIDENTES DE SEGURIDAD.

Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

Ante la detección de eventos de seguridad individuales o simultáneos que constituyan situaciones potenciales de violación a la seguridad de la información, se requiere adelantar actividades de análisis, contención y respuesta para controlar e impedir estos potenciales ataques.

Las actividades incluidas dentro de la gestión de los incidentes son:

- Definición de criticidad y catalogación de incidentes para que responda adecuadamente a los requerimientos.
- Coordinar las pruebas y ejecución de las acciones de respuesta a incidentes de seguridad, contención y recuperación junto con el equipo de expertos de Alcaldía de Santiago de Cali, administradores de plataforma y terceros involucrados en el incidente.
- Al momento de darse un evento o incidente de nivel medio o alto, dentro de las recomendaciones debe presentarse un informe de resolución de fallas (Root cause analysis).

De igual manera se requiere del siguiente personal idóneo, que pueda prestar atención a incidentes 7X24 con prioridades; baja, media, alta y muy alta:

CARGO	**PERFIL**	**Cantidad de personas**	**FUNCIONES**
Gerente de Proyecto	Profesional en ingeniería con Máster en gestión de informática y telecomunicaciones. 12 años de Experiencia en proyectos a partir de la Tarjeta profesional. Certificaciones	1	Responsable de asesorar y dar claridad en temas funcionales y de procesos: están a su cargo todas las definiciones y aprobaciones de tipo funcional.

	• Project Management Professional PMP Project Management- Vigente • Certificación ITIL 4 Managing Professional. • Certificación Lead Cybersecurity Professional • Certificación Cobit Fundamentos 2019 • Certificación Auditor Interno en Sistemas de Gestión de Seguridad de la Información ISO 27001 • Certificación SCRUM MASTER PROFESIONAL CERTIFICATE(SMPC). • Certificación Desarrollo de Auditorías internas • Certificación SIX sigma – White Belt • Aspectos Basicos de Seguridad de AWS		Escalar decisiones que se salgan de su conocimiento o ámbito, y traer al proyecto las respuestas finales de manera oportuna. Articular y coordinar las actividades a ejecutar por el equipo del proyecto.
Especialista Senior en seguridad	Profesional en ingeniería de sistemas, electrónica, telecomunicaciones o afines, con Máster en gestión de informática y/o telecomunicaciones. 10 años de Experiencia en proyectos de Seguridad Informática y protección de datos personales (Ley 1581 de 2012). Certificaciones: • Auditor Lider ISO 27001:2013 • Implementador Líder ISO 27001:2013 • COBIT 5 • CISM • Auditor Lider ISO 31000 • Auditor Lider ISO 22301 • CISA • CSX • Cybersecurity Manager • Scrum Master	1	Responsable de asesorar y dar claridad en temas funcionales y de procesos: están a su cargo todas las definiciones y aprobaciones de tipo funcional. Escalar decisiones que se salgan de su conocimiento o ámbito, y traer al proyecto las respuestas finales de manera oportuna. Velar y garantizar que se prueben todos los escenarios necesarios de la administración organizacional y datos maestros de personal, finalicen estado exitoso.
Especialista en seguridad de la información	Ingeniero de sistemas, o afines con Magister en seguridad de la información.	1	Profesional encargado de ejecutar las actividades del contrato

	10 años de Experiencia en proyectos de seguridad de la información. Certificaciones: • CISM • CISSP • CEH • ECIH • Auditor Lider ISO 27001 2022		
Especialista Senior en pentesting	Profesional en ingeniería de sistemas o fines, con especialización en seguridad informática o de la informacion. 10 años de Experiencia en proyectos de seguridad de la información Certificaciones • CISSP • CISM • CEH • CHFI • ECSA • CNFE • CIHE • CSA	1	Profesional encargado de ejecutar las actividades del contrato
Especialista en pentesting	Profesional en ingeniería de sistemas o afines, con Especialista en seguridad de la información o seguridad informática. 3 años de experiencia en proyectos de seguridad de la información • Certificado en CEH	1	Profesional encargado de ejecutar las actividades del contrato
Ciberseguridad Junior	Profesional en ingeniería de sistemas o afines. Dos años de experiencia en proyectos de seguridad de la información Certificación • Auditor líder ISO 27001 2022	1	Profesional encargado de ejecutar las actividades del contrato
TOTAL, PERSONAL	6 PERSONAS		