**Consultoría para la Gestión de Crisis**

**Proyecto**

Gestión de Crisis – Sospecha de ataque de Ransomware

### Necesidades del Cliente

* + - Identificar situación actual en segmento de red
    - Identificar posibles amenazas en el Servidor afectado (correo electrónico)
    - Identificar posibles vulnerabilidades de seguridad

### Propuesta de Servicios Totalsec

De acuerdo al requerimiento del cliente, recomendamos los siguientes servicios:

##### SITUACIÓN ACTUAL

Se lleva a cabo sesión de entendimiento del problema reportado por el Cliente:

* + - Sospecha de servidor de correo posiblemente afectado
    - Un usuario del área contable está recibiendo ransomware a través de su correo electrónico y tiene afectación en el performance de su equipo

##### RECOMENDACIÓN DE SERVICIO

Se recomienda realizar una **Gestión de Crisis** que se describe a continuación:

El servicio de Respuesta a Incidentes, tiene como objetivo la gestión del incidente y/o incidente crítico reportado por el CLIENTE con el fin de apoyar en la mitigación de cualquier incidente de Seguridad sobre la infraestructura tecnológica y de comunicaciones reportado del CLIENTE.

Para poder brindar el servicio de Respuesta a Incidentes de Seguridad, será necesario tener acceso a pantallas o Dashboards, Logs de actividad de la infraestructura reportada por el Cliente, así como a los repositorios de Logs o de correlacionador de eventos o en su defecto el poder tener acceso al menos a 1 ingeniero especializado que conozca la infraestructura y procesos de negocio del ecosistema y que pueda proporcionar datos necesarios para realizar la contención del evento reportado.

Este servicio incluye:

* + - * Gestión de respuesta a Incidente - Análisis
      * Consultoría de Mitigación del Evento - Contención
      * Reporte final de análisis con línea de tiempo con puntos revisados y contención ejecutada.

**ESTE SERVICIO DE GESTIÓN DE CRISIS CONSISTE EN UNA BOLSA DE 50 HORAS INCIALES, EN CASO DE REQUERIR HORAS ADICIONALES PARA LA EJECUCIÓN DE ACTIVIDADES, SE PODRÁN COBRAR DE MANERA ADICIONAL A LA PRESENTE PROPUESTA.**

**PROCESO DE ATENCION**

* + - * Totalsec evaluará la solicitud de atención a evento de seguridad reportada por el CLIENTE y realiza la priorización y clasificación conforme al siguiente apartado:

**Baja**: Es un suceso o serie de sucesos que por las características que tiene no representa un riesgo en la operación adecuada de los servicios, sin embargo, requiere de revisión por parte de Totalsec.

**Media**: Es un suceso o serie de sucesos que por las características que tiene, puede representar un riesgo o afectación en la Seguridad informática del CLIENTE.

**Alta**: Es un suceso o serie de sucesos que por las características que tiene, representa un riesgo en la Seguridad, o tiene una probabilidad alta de afectación en la seguridad informática del CLIENTE.

**Persistente**: Es un suceso que ocurre cuando se tiene algún puerto o servicio conocido como vulnerable de una alerta previamente emitida y se continúan recibiendo ataques al mismo servicio/puerto.

**Crisis**: Suceso o condición en el que un sistema, servicio o red se detecta una violación de seguridad, poniendo en peligro las propiedades (integridad, disponibilidad y confidencialidad) de la información

* + - * Una vez que Totalsec realice el dictamen del incidente reportado y determine no clasificarlo como incidente Crítico, Alto o Persistente, las horas tomadas para realizar este dictamen, serán descontadas de las horas ofertadas para este servicio.
      * Ante una Crisis confirmada por Totalsec o el CLIENTE, se conformará un Equipo de Respuesta a Incidentes de Seguridad de Tecnología de la Información (ERIST) para la gestión de la crisis, este estará conformado por los siguientes perfiles:
      * 1 Lider del ERIST.
      * 1 Coordinador del ERIST.
      * 1 Especialista en Aplicaciones.
      * 1 Especialista en Redes.
      * 1 Especialista en Endpoints.

Este equipo será el responsable de la gestión de la crisis donde:

Será responsabilidad del Coordinador del ERIST mantener informado al cliente sobre el seguimiento de la Crisis de seguridad presentada, incluyendo los reportes al finalizar el día en Crisis de seguridad que ya no presenten afectación pero que sigan abiertas para su posterior análisis.

El seguimiento y cambio de estatus ante el cliente de las Crisis de seguridad e Incidente Mayor que duren más de 1 día se realizará de la siguiente manera:

1. Para las primeras 24 horas se realizarán notificaciones cada 90 minutos a través de los medios definidos.
2. Pasando las primeras 24 horas naturales se elaborará y entregará un informe diario de actividades realizadas al cliente.

Toda Crisis de Seguridad e Incidente quedará documentada desde su informe inicial,

Contención, análisis, cierre y hasta su reporte final que se deberá entregar en un plazo no mayor a 48 horas naturales posteriores al cierre.

Una vez declarada Crisis o Incidente Mayor no deberá tomar más de 3 Hrs. para confirmar o descartar el mismo.

**EQUIPO DE TRABAJO (INICIAL)**

* 1 Especialista en Hacking Ético y programación de código seguro (ecosistema de aplicativos)
* 1 Project Manager Certificado

##### CONSIDERACIONES ESPECIALES

* Se podrá cotizar al cliente, de manera independiente a este documento, cualquier necesidad de tecnología o de consultoría de seguridad de la información que resulte de los análisis realizados a la información e infraestructura tecnológica
* El CLIENTE deberá de proporcionar un acceso físico o remoto a TOTALSEC para poder realizar los análisis de los eventos de seguridad en los dispositivos de seguridad del CLIENTE, en su defecto proporcionar todos los logs, eventos, indicios, diagramas, configuraciones etc; a TOTALSEC para poder apoyar con las actividades de contención de los eventos de seguridad y la realización del análisis forense.
* El CLIENTE identificará y facilitará al personal adecuado para otorgar las facilidades con sesiones o documentación que TOTALSEC necesite o requiera.
* El CLIENTE proporcionará a TOTALSEC el listado de los activos de información, características y diagramas de los componentes del ecosistema, para la mejor atención de los incidentes.

**BENEFICIOS**

* Información de Ransomware o algún otro tipo de afectación que se tenga.
* Información de Vulnerabilidades en el Segmento Principal, así como en los activos que estén conectados sobre VPN
* Información de cómo evitar afectaciones.
* Informacion para mejorar el control de seguridad en segmento de red.

##### Para lograr el cumplimiento y éxito del Proyecto, será necesario por parte del Cliente:

* Reforzar el compromiso de la dirección del Negocio para el cumplimiento del objetivo del proyecto
* Concientizar al personal clave involucrado sobre los beneficios que el proyecto aportará al Negocio
* Entrega en tiempo y forma de Información requerida al Cliente con la finalidad de evitar retrasos en el proyecto

##### Facilidades para Totalsec:

* Firma de NDA (Non- disclosure agreement) con los responsables del Proyecto con la finalidad de tener acceso a la información necesaria del Negocio y así conservar su confidencialidad
* Listado de personal clave para llevar a cabo las entrevistas y análisis
* EL CLIENTE deberá coordinar y facilitar los recursos necesarios para el proyecto
* Todos los servicios se ejecutarán de manera remota por contingencia COVID-19
* En caso de ser necesario hacer visita presencial la propuesta ya cuenta con los viáticos necesarios

### Entregables

* + - Reporte final con recomendaciones macro por cada fase del Proyecto de Gestión de Crisis
* Informe de Gestión del Incidente.
* Reportes de Crisis de Seguridad.