|  |  |
| --- | --- |
| **ELABORADO POR** | |
| **Nombre del Especialista TI:** | **Rol:** |
| **Fecha del Informe: *dd/mm/aa*** | **Correo Electrónico:** |
| **Gestión de Conocimiento: *Código asignado*** | **No. Caso: *Número de caso registrado en la herramienta de gestión.*** |

|  |  |
| --- | --- |
| 1. **INFORMACIÓN DEL INCIDENTE** | |
| **Tipo Incidente**  Estándar\_\_\_  Masivo\_\_\_ | **Tipo de Incidente: *(De acuerdo con la matriz de categorización)*** |
| **Incidente:** ***Si es incidente de Seguridad, por favor describir el evento de acuerdo con la lista del numeral 7.2.1 del procedimiento SC05-P01.***  ***El análisis de la causa raíz de la afectación*** | |
| **Descripción del Incidente: *(Información del caso registrado en la herramienta de gestión)*** | |

| **RECOLECCIÓN DE EVIDENCIAS** |
| --- |
| ***Se debe anexar la evidencia relacionada y recolectada en cada una de las fases.*** |

|  |  |
| --- | --- |
| 1. **DETECCIÓN DEL INCIDENTE** | |
| **Fecha y Hora de Detección:**  ***monitoreo-software*** | **Fecha y Hora de validación del incidente:**  ***Gestión primaria por parte de TI*** |
| **Fecha y Hora de inicio del incidente:**  ***por herramientas o reportado por el usuario ante el CSIT*** | **Fuente de Detección:**  ***usuario, administrador, sistema*** |
| **Persona que reporta:**  ***Nombre del usuario o del administrador*** | **Áreas de la entidad afectadas:**  ***Oficinas - Jefaturas – Grupos- Personas*** |
| **Activos Afectados:**  ***Equipos-Información-Personas*** | **Fecha y hora de comunicación del incidente a Seguridad de la Información:**  ***Al oficial de seguridad o delegado*** |
| **Descripción de la Detección: *(Información del caso registrado en la herramienta de gestión)*** | |

| **RECOLECCIÓN DE EVIDENCIAS** |
| --- |
| ***Se debe anexar la evidencia relacionada y recolectada en cada una de las fases.*** |

|  |  |
| --- | --- |
| 1. **CONTENCIÓN DEL INCIDENTE** | |
| **Fecha del inicio de la contención:**  ***inicio de gestión por parte del especialista*** | **Hora del inicio de la contención:**  ***inicio de gestión por parte del especialista*** |
| **Quien autoriza las acciones:**  ***Profesional o delegado de la OTI*** | **Quien ejecuta las acciones:**  ***Especialista o grupo a cargo de la gestión del incidente*** |
| **Descripción de las acciones de contención: *(Información del caso registrado en la herramienta de gestión)*** | |
| **Resultados de las acciones:**  ***Si los resultados no son efectivos se documentan todos los intentos de contención llevando los mismos campos.)*** | |

| **RECOLECCIÓN DE EVIDENCIAS** |
| --- |
| ***Se debe anexar la evidencia relacionada y recolectada en cada una de las fases.*** |

|  |
| --- |
| 1. **REMEDIACIONES Y CAMBIOS** |

|  |  |
| --- | --- |
| **Fecha del inicio de la remediación o cambio:** | **Hora del inicio de la remediación o cambio:**  ***Si aplica*** |
| **Quien autoriza las acciones:**  ***Profesional o delegado de la OTI*** | **Quien ejecuta las acciones:**  ***Especialista o grupo a cargo de la gestión del incidente*** |
| **Descripción de las acciones de remediación o cambios aprobados:** | |
| **Resultados de las acciones:** | |

| **RECOLECCIÓN DE EVIDENCIAS** |
| --- |
| ***Se debe anexar la evidencia relacionada y recolectada en cada una de las fases.*** |

|  |  |
| --- | --- |
| 1. **CIERRE DEL INCIDENTE** | |
| **Fecha**: ***Fecha en la que sucede/descubre la incidencia*** | **Proveedor:**  ***Datos y caso creado con el proveedor si la incidencia tuviese relación con uno.*** |
| **Producto:**  ***Selección del producto/servicio relacionado con la incidencia*** | **Tipo de impacto: *según numeral 7.2.3 del procedimiento SC05-P01***  **\_\_ Confidencialidad o Privacidad**  **\_\_ Integridad**  **\_\_ Disponibilidad** |
| **Severidad - grado de impacto: *según numeral 7.2.3 del procedimiento SC05-P01):***  **\_\_\_ Alta**  **\_\_\_ Media**  **\_\_\_ Baja**  **\_\_\_ Desconocida** | **Áreas de la entidad afectadas: *área de la organización afectada por la incidencia*** |
| **Notifica: *Personal que notifica la incidencia*** | **Notificación: *Fecha en la que se notifica la incidencia*** |
| **Registra: *Personal que registra*** | **Registro: *Fecha en la que se registra la incidencia*** |
| **Solución: *Descripción de la solución (temporal o definitiva) o acción correctiva aplicada para dar solución a la incidencia y lecciones aprendidas*** | |
| **Resultados de las acciones:**  ***Si los resultados no son efectivos se documentan todos los intentos de contención llevando los mismos campos.)*** | |
| **Conclusiones:** | |
| **Recomendaciones:** | |

| **RECOLECCIÓN DE EVIDENCIAS** |
| --- |
| ***Se debe anexar la evidencia relacionada y recolectada en cada una de las fases.*** |

|  |  |
| --- | --- |
| 1. **MEJORAS**   Describir los cambios en los controles, políticas, procedimientos, formatos y mecanismos que estén orientados a prevenir incidentes similares o relacionados. | |
| **Responsables:** | **Tipo: *cambio de arquitectura, nuevas o modificación en reglas, cambios en configuraciones, actualizaciones, otros.*** |
| **Activos: *Listar el hardware o software sobre el cual se requiere el cambio*** | **Criticidad: *Urgencia del cambio (muy alto, alto, medio, bajo) de acuerdo con lo indicado en la herramienta de gestión.*** |
| **Gobierno: *cambios en políticas, procedimientos, instructivos, formatos o manuales*** | |
| **Descripción:** | |

| **RECOLECCIÓN DE EVIDENCIAS** |
| --- |
| ***Se debe anexar la evidencia relacionada y recolectada en cada una de las fases.*** |

|  |
| --- |
| 1. **LECCIONES APRENDIDAS** |
| **Describir exactamente qué sucedió, en qué momento y cómo el personal gestionó el incidente:** |
| **Se tomaron las medidas o acciones que facilitaron la recuperación eficiente:** |
| **Cuál debería ser la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar:** |
| **Las acciones correctivas que puedan prevenir incidentes similares en el futuro:** |
| **Cuáles herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro:** |

| **RECOLECCIÓN DE EVIDENCIAS** |
| --- |
| ***Se debe anexar la evidencia relacionada y recolectada en cada una de las fases.*** |

|  |
| --- |
| **POSTULACIONES** |
| **¿Se debe postular a la Gestión de Problemas con el fin de iniciar proceso para verificación de análisis de causa raíz o creación de Error conocido?:**  **\_\_\_ Error Conocido \_\_\_ Análisis Causa Raíz**  **\_\_\_ SI \_\_\_ NO**  **¿Por qué? *Si la respuesta es NO justidicar por que*** |
| **¿Se debe postular a la gestión de conocimiento la solución de este Incidente? *Sí la solución es definitiva, se debe postular a conocimiento***  **\_\_\_ SI \_\_\_ NO**  **¿Por qué? *Si la respuesta es NO justificar por que*** |
| **¿Se ejecutó algún RFC antes o después del Incidente?**  **\_\_\_ SI \_\_\_ NO**  **¿Cuál? *Número de cambio registrado en la herramienta de gestión*** |

|  |  |
| --- | --- |
| **DOCUMENTOS RELACIONADOS**  *En este capítulo se relacionan los documentos del SIGI que se utilizan para ejecutar las actividades contenidas en el documento. Cuando se hace referencia a un documento del SIGI se relaciona el nombre del documento seguido del código* | |
| **Nombre del Documento:** | **Ubicación/URL:** |

|  |  |
| --- | --- |
| **DOCUMENTOS EXTERNOS**  *En esta sección se relacionan los documentos emitidos por una entidad externa. los cuales son relevantes para el Sistema de Gestión de Calidad; Los ejemplos de los emisores pueden ser: clientes, proveedores, legisladores, reguladores, organismos de control* | |
| **Nombre del Documento:** | **Ubicación/URL:** |