|  |
| --- |
| **REPORTE Y NOTIFICACIÓN DEL INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** |
|  |
| Número de Ticket Asignado al Incidente |  |  |
|  |  |  |  |  |  |  |  |
| Fecha y Hora Reporte de Incidente de Seguridad de la Información |  |  |
|  |
|  |
| Nombre y Área Quien Reporta el Incidente |  |  |
|  |  |  |  |  |  |  |  |
| **DESCRIPCIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** |
| 1. **DETECCIÓN Y NOTIFICACIÓN**
 |
| ¿Qué Sucedió?: |
|
| ¿Cómo Sucedió?: |
|
| ¿Por qué Sucedió?: |
|
| ¿Tipo de activo afectado y cual fue?:C:\Users\JLCARR~1\AppData\Local\Temp\msohtmlclip1\01\clip_image001.pngHardware ¿Cuál fue el Activo afectado?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ C:\Users\JLCARR~1\AppData\Local\Temp\msohtmlclip1\01\clip_image001.pngSoftwareC:\Users\JLCARR~1\AppData\Local\Temp\msohtmlclip1\01\clip_image001.pngInformaciónC:\Users\JLCARR~1\AppData\Local\Temp\msohtmlclip1\01\clip_image001.pngServicioC:\Users\JLCARR~1\AppData\Local\Temp\msohtmlclip1\01\clip_image001.pngComponente de red |
|
| C:\Users\JLCARR~1\AppData\Local\Temp\msohtmlclip1\01\clip_image001.pngC:\Users\JLCARR~1\AppData\Local\Temp\msohtmlclip1\01\clip_image002.pngC:\Users\JLCARR~1\AppData\Local\Temp\msohtmlclip1\01\clip_image002.png¿Nivel del incidente?: ALTO MEDIO BAJO |
|
|
| C:\Users\JLCARR~1\AppData\Local\Temp\msohtmlclip1\01\clip_image002.pngC:\Users\JLCARR~1\AppData\Local\Temp\msohtmlclip1\01\clip_image001.png¿Se identifica responsable del Incidente?: SI NO Cual? |
|

|  |
| --- |
| 1. **ANALISIS PRELIMINAR**
 |
| Análisis Técnico del Incidente:*(Es importante que el Analista que recibe la solicitud, trate de recolectar con la mayor información posible, antes de escalar el caso a seguridad de la información. Se deben tener en cuenta las Instrucciones para la priorización y categorización de incidentes de seguridad de la información – GDI-TIC-IN016).* |

|  |
| --- |
| 1. **CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN**
 |
| CONTENCIÓN: *(Qué actividades se llevaron a cabo para realizar la contención del incidente.)* |
| ERRADICACIÓN:*(Qué actividades se llevaron a cabo para realizar la erradicar el incidente.)* |
| RECUPERACIÓN:*(Qué actividades se llevaron a cabo para realizar la recuperación del incidente.)* |

|  |
| --- |
| 1. **INVESTIGACIÓN DEL INCIDENTE**
 |
| “Recolección de datos – recolección de evidencia”*Es importante que el Analista investigue y documente un resumen de la evidencia relacionada con el incidente de seguridad de la información* |

|  |
| --- |
| 1. **LECCIONES APRENDIDAS**
 |
| *Es importante que el Analista o especialista documente lo aprendido, de forma tal que no se vuelva a presentar el incidente en el futuro o si se presenta, se pueda solucionar de una manera muy rápida y eficiente.* |

|  |
| --- |
| 1. **PLAN DE ACCION**
 |
| responsables de cerrar brechas – en la siguiente tabla

|  |  |  |  |
| --- | --- | --- | --- |
| Acción | Responsable | Fecha inicio | Fecha fin |
|  |  |  |  |

 |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Director de Tecnologías e Información**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Responsable de seguridad de la información**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Responsable de Infraestructura**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Responsable de mesa de servicios**