|  |
| --- |
| **Formato de Registro de Incidente de Seguridad de la Información** |
| **Identificación del incidente** |
| Fecha del incidente (DD-MM-AAAA) |   |
| Número de incidente de seguridad(asigna herramienta de mesa de servicios) | (Por favor reportar en PROACTIVA NET para realizar seguimiento allí) |
|  |
| Detalles de quien reporta / identifica el incidente de seguridad de la información |
| Nombre | Correo electrónico  |
| Teléfono  | Dependencia / Organización  |
| Detalles del funcionario del primer respondiente del incidente |
| Nombre  | Correo electrónico  |
| Teléfono | Dependencia / Organización  |
| **Descripción del incidente** |
| ¿Qué ocurrió?: *(describa los hechos que se reportaron al momento de identificar el incidente)* |
|  |
| ¿Cómo ocurrió?: *(describa la forma como se presume o se concluye que generó el incidente de seguridad de la información* |
|  |
| ¿Por qué ocurrió?: *(a partir de los resultados de la investigación o el análisis de causa raíz explique las razones por las cuales ocurrió el incidente)* |
|  |
| ¿Qué elementos están afectados?: *(describa los activos de información que fueron afectados por el incidente de seguridad de la información)* |
|    |
| ¿Qué impactos se perciben?: *(evalúe como se impactaron la confidencialidad, integridad o disponibilidad de los activos de información afectados directa o indirectamente por el incidente)* |
|  |
| ¿Existe alguna vulnerabilidad identificada?: *(si se detectan vulnerabilidades que permitieron la ocurrencia del incidente, descríbalas)* |
|    |
| **Información de tiempo del incidente de seguridad** |
| Fecha y hora en que se reportó el incidente |   |
| Fecha y hora en que se descubrió el incidente |   |
| Fecha y hora en que ocurrió el incidente *(puede indicar un instante estimado si no existe información precisa)* |   |
| ¿El incidente ya finalizó?  | SI  | No  |
| En caso afirmativo, describa cuanto duró el incidente |
|   |

|  |
| --- |
| **Categorización y priorización de incidentes** |
| **En caso de desastre natural indique**Terremoto \_\_ Inundación \_\_ Viento fuerte \_\_\_ Descarga eléctrica \_\_\_ Derrumbe Otro\_\_\_\_ ¿cuál? \_\_\_\_ | **En caso de disturbio civil indique**Ataque terrorista \_ Asonada \_\_ Otro\_\_\_\_ ¿cuál? \_\_\_\_\_\_\_\_\_\_ |
| **En caso de daños físicos indique:**Incendió \_\_ Daño por agua\_\_ Contaminación química \_\_\_ electrostática \_\_\_\_Destrucción de equiposDestrucción de medios\_\_\_\_ Robo de equipos \_\_\_ Robo de medios \_\_ Pérdida de equipos \_\_ Pérdida de medios \_\_\_ Alteración de equipos \_\_\_\_ Alteración de Medios \_\_\_\_ Otro\_\_\_\_\_ ¿cuál? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **En caso de fallas a infraestructura indique**Falla de alimentación eléctrica \_\_\_\_ Falla en redes de telecomunicaciones \_\_\_\_Falla en aire acondicionado \_\_\_\_Falla en suministro de agua \_\_\_\_ Otro\_\_\_\_ ¿cuál? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **En caso de falla técnica indique**Falla de hardware \_\_\_\_\_ Mal funcionamiento de software \_\_\_\_ Sobre carga de sistema \_\_\_\_ Otro\_\_\_ ¿cuál? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **En caso de software malicioso indique:**Gusano de red \_\_\_ Troyano \_\_\_\_ Virus \_\_\_\_\_ Sitio web con malware \_\_\_ Otro\_\_\_\_\_ ¿cuál? \_\_\_\_\_\_\_\_\_\_\_ |
| **En caso de ataque informático indique:**Escaneo de puertos\_\_\_\_ Explotación de vulnerabilidad\_\_\_\_ Uso de puertas traseras \_\_\_\_\_Intento de acceso\_\_\_ Denegación de servicio\_\_\_ Otro\_\_\_\_ ¿cuál? \_\_\_\_\_\_\_\_ | **En caso de violación de reglas indique**:Uso no autorizado de sistema/equipo/activo \_\_Violación de derechos de autor \_\_\_\_Incumplimiento de política de seguridad \_ Otro\_\_\_¿cuál? \_\_\_\_\_\_\_\_\_\_\_ |
| **En caso de puesta en peligro de funciones indique:**Abuso de derechos \_\_ Falsificación de derechos \_\_\_ Operaciones incorrectas\_\_\_ Otro\_\_\_\_¿cual? \_\_\_\_\_\_\_\_\_\_ | **En caso de puesta en peligro de la información indique**:Interceptación \_\_\_\_ Espionaje \_\_\_\_ Chuzada de teléfono \_\_\_\_ Divulgación \_\_\_\_ Ingeniería social \_\_\_ Phishing \_\_\_\_ Robo de datos \_\_\_\_ Pérdida de datos \_\_\_ Alteración de datos \_\_Errores en datos \_\_\_ Análisis de tráfico \_\_\_Otro\_\_\_ ¿cuál? |
| **En caso de contenido peligroso indique**:Contenido ilegal \_\_\_\_ Contenido amenazador \_\_\_Contenido malicioso \_\_\_ Contenido abusivo\_\_\_Otro\_\_\_\_ ¿Cuál? \_\_\_\_\_\_\_ | **¿Otros? Describa** |

|  |
| --- |
| **Valoración de impacto** |
| Componentes afectados |
| Información (describa) | Software (describa) |
| Hardware (describa) | Comunicaciones (describa) |
| Procesos (describa) | Otros (describa) |
| Resultado de la valoración de impacto de incidente de acuerdo con la metodología de gestión de riesgos institucional |
| Impacto en confidencialidad |  |
| Impacto en integridad |  |
| Impacto en disponibilidad |   |

|  |
| --- |
| **Resolución del incidente** |
| Fecha de inicio de la investigación del incidente:  |  |
| Nombres de los investigadores del incidente  |  |
| Fecha de finalización del incidente  |  |
| Fecha de finalización de la investigación |  |
| Detalles de la ubicación de reportes y evidencias de la investigación: buzones de correo.  |   |
| Si el incidente fue causado por personas indique. | Persona \_\_\_ Organización/institución establecida legalmente\_\_\_ Grupo organizado\_\_\_\_ Accidente \_\_\_\_ No hay Autor identificado \_\_\_\_ |
| Detalles descriptivos del autor:  |
| Motivación real o percibida para realizar la acción indique: | Retribución económica \_\_\_ Pasatiempo \_\_\_\_\_\_\_\_\_\_\_\_ Piratería \_\_\_\_\_\_Política/Terrorismo\_\_\_\_\_ Venganza \_\_\_\_ Otro ¿Cuál? \_\_ \_ |
| **Acciones realizadas para tratar el incidente:** |
| Acciones de identificación |
|    |
| Acciones de Contención |
|   |
| Acciones de Retiro de falla |
|   |
| Acciones de recuperación |
|   |
| Acciones pendientes |
|  |
| Otras acciones |
|   |

|  |
| --- |
| **Conclusión y cierre del incidente** |
| Lecciones aprendidas |
| Fue bueno el desempeño del grupo de atención de incidentes. | Aclaraciones:  |
| Fue bueno el desempeño del grupo directivo de la entidad | Aclaraciones:  |
| Se ejecutaron pasos o acciones que pudieron impedir la recuperación | Aclaraciones:  |
| Se siguieron los procedimientos documentados | Aclaraciones:  |
| Fueron adecuados los procedimientos | Aclaraciones:  |
| Qué acciones se deben mejorar |
| **Notificaciones** |
| Personal Interno que fue notificado |
| Directores \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Responsables de procesos \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Responsables de sistemas de información \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Funcionario que reporto el evento \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Personal externo que fue notificado (marque con X) |
| Centro Cibernético de la Policía | Col CERT | Comando Conjunto Cibernético | CSIRT Gobierno |
| Delegatura de protección de datos personales | Procuraduría | Otros |

Firmas

|  |  |  |
| --- | --- | --- |
| Elaboró  | Revisó | Aprobó |