## REPORTE INICIAL DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

1. **Datos de quién reporta:**

| | |
|---|---|
| Nombre de la institución que reporta: | |
| Nombre y cargo de la persona que reporta: | |
| Correo electrónico: | |
| Teléfono: | |
| Áreas a quienes ha sido reportado el incidente en la institución | |

2. **Información General del Incidente:**

| **Información del Incidente** | |
|---|---|
| 2.1. Fecha y hora del Incidente: | |
| 2.2. Fecha y hora de detección: | |
| 2.3. Breve descripción del incidente (¿qué pasó?, ¿dónde pasó?, ¿cuándo pasó?, ¿cómo pasó?, ¿Qué servicios y como se afectaron?) | |
| 2.4. Componentes de la Infraestructura Tecnológica afectados en el incidente de seguridad de la información. | ☐ Zona de red afectada (internet, red interna, red de administración, entre otras): _____ |
| | ☐ Tipo de sistema afectado (servidor de archivos, servidor web, servicio de correo, base de datos, estaciones de trabajo, ya sea de escritorio o móvil, entre otros): _____ |
| | ☐ Sistema operativo (especificar versión): _____ |
| | ☐ Protocolos o servicios y aplicaciones (especificar versión): _____ |
| | ☐ Otro: Especificar_____ |
| | |

| Información del Incidente | |
|---|---|
| 2.5. Canales de atención a clientes afectados por el incidente y estimación inicial de número de puntos de atención o porcentaje de afectación: | ☐ TPV |
| | ☐ Sucursales |
| | ☐ Portal Web / Móvil |
| | Estimación inicial: _____ |
| 2.6. Instalación afectada: | ☐ Centro de Datos |
| | ☐ Oficinas de servicio<br>Oficina matriz |
| | ☐ Sucursal |
| | ☐ Proveedor<br>Otro: _____ |
| 2.7. Nivel estimado de daño o impacto provocado por el incidente de seguridad de la información: | **Crítico; porque: _____**<br>**Medio**<br>**Bajo** |
| 2.8. Detallar las acciones inmediatas que han realizado para mitigar el incidente de seguridad de la información: | |

**3. Clasificar el incidente de seguridad de la información reportado en el presente anexo con base en las siguientes definiciones:**

| Clases de Incidente | Aplica | Describir el incidente específico |
|---|---|---|
| 3.1. Ataques físicos (deliberados o intencionales) tales como: sabotaje, vandalismo, robo de dispositivos, fuga de información en medios físicos, acceso físicos no autorizados, coerción, extorsión, ataque terrorista, entre otros. | ☐ | |
| 3.2. Daño no intencional o accidental, pérdida de información o pérdida de activos, tales como: información compartida indebidamente, errores u omisiones en sistemas o dispositivos, errores en procedimientos o controles, cambios indebidos a datos, extravío de información o dispositivos, entre otros. | ☐ | |
| 3.3. Incidentes por desastres naturales o ambientales, tales como: Terremotos, inundaciones, huracanes, incendios, radiación, corrosión, explosiones, entre otros. | ☐ | |
| 3.4. Incidentes por fallas o mal funcionamiento, tales como: Falla en dispositivos o sistemas, fallas en comunicaciones, en servicios o equipos de | ☐ | |

| | Clases de Incidente | Aplica | Describir el incidente específico |
|---|---|---|---|
| | terceros o en la cadena de suministros, entre otros. | | |
| 3.5. | Incidentes por la interrupción o falta de insumos, tales como: Ausencia de personal, huelgas, interrupción de servicios de energía, agua, telecomunicaciones, entre otros. | ☐ | |
| 3.6. | Incidentes por intercepción de datos, tales como: espionaje, intercepción de mensajes, wardriving, ataques de hombre en medio, secuestro de sesiones, programas sniffers, robo de mensajería, entre otros. | ☐ | |
| 3.7. | Incidentes por actividad maliciosa (ciber ataques) con el fin de tomar el control, desestabilizar o dañar un sistema informático, tales como: Robo de identidad, Phishing, Negación de servicio (DOS, DDOS), Código malicioso (malware, troyanos, gusanos, inyección de código, virus, ransomware), Ingeniería Social, Vulneración de certificados (suplantación de sitios, certificados falsos), manipulación de hardware (proxies anónimos, skimmers, sniffers), alteración de información (suplantación de direccionamiento y tablas de ruteo, DNS poisoning, alteración de configuraciones), abuso de aplicaciones de auditoría, ataques de fuerza bruta, abuso de autorizaciones, entre otros. | ☐ | |
| 3.8. | Originadas por aspectos legales, tales como: Violación de cláusulas y acuerdos, violación de confidencialidad, decisiones adversas (resoluciones judiciales en la misma jurisdicción o en otras), entre otras. | ☐ | |