FORMULARIO DE REGISTRO DE INCIDENTE DE SEGURIDAD

ID del Incidente: INC-SEC-_____-_____
Fecha de creación: //___ Hora: *:*

SECCIÓN 1: INFORMACIÓN BÁSICA

Reportado por:
☐ **Usuario final**
☐ **Sistema automático (Antivirus/IPS)**
☐ **Monitoreo (Graylog)**
☐ **Equipo de TI**
☐ **Otro: _____**

Nombre del reportante:
_____
Email: _____ Ext: _____

Fecha/Hora del incidente: //_____ *:*

Fecha/Hora de detección: //_____ *:*

SECCIÓN 2: CLASIFICACIÓN

Tipo de incidente:
☐ **Malware (especificar): _____**
☐ **Phishing**
☐ **Ransomware**
☐ **Acceso no autorizado**
☐ **Compromiso de credenciales**
☐ **Exfiltración de datos**
☐ **Denegación de servicio**
☐ **Actividad maliciosa (especificar):**

_____

☐ **Otro: _____**

Severidad inicial:

☐ **CRÍTICO - Afectación masiva o sistemas críticos**
☐ **ALTO - Afectación significativa**
☐ **MEDIO - Impacto limitado**
☐ **BAJO - Mínimo impacto**

SECCIÓN 3: SISTEMAS/USUARIOS AFECTADOS

Equipos afectados:

Nombre de equipo	IP Address	MAC Address	Usuario	Ubicación

Servicios afectados:

☐ **Correo electrónico (Zimbra)**
☐ **Active Directory**
☐ **Servidor de archivos**
☐ **Aplicación crítica: _____**
☐ **Red/Firewall**
☐ **VPN**
☐ **Otro: _____**

Usuarios afectados: _____ usuarios aproximadamente

¿Datos sensibles involucrados?

☐ **Sí** ☐ **No** ☐ **En investigación**

Tipo de datos:

☐ **Información personal**
☐ **Información financiera**
☐ **Información clasificada**

☐ **Credenciales**
☐ **Otro: _____**

SECCIÓN 4: DESCRIPCIÓN DEL INCIDENTE

Descripción detallada:

¿Cómo se detectó?

Síntomas observados:
☐ **Lentitud del sistema**
☐ **Comportamiento inusual de aplicaciones**
☐ **Archivos encriptados**
☐ **Pérdida de acceso a archivos**
☐ **Mensajes de error inusuales**
☐ **Actividad de red sospechosa**
☐ **Alertas del antivirus**
☐ **Correo sospechoso**
☐ **Otro: _____**

SECCIÓN 5: INDICADORES DE COMPROMISO (IOCs)

Archivos maliciosos:IPs sospechosas:

Nombre del archivo	Ubicación	Hash (SHA256)	Acción

IP Address	Puerto	Tipo de conexión	Bloqueada (S/N)

Dominios sospechosos:

Dominio	Relacionado con	Bloqueado (S/N)

URLs maliciosas:

_____

_____

Cuentas comprometidas:

Usuario	Dominio	Acciones tomadas

_____

SECCIÓN 6: ACCIONES INMEDIATAS TOMADAS

Fecha/Hora: //_____ :

☐ **Equipo aislado de la red**
☐ **Cuenta de usuario bloqueada**
☐ **IP/Dominio bloqueado en firewall**
☐ **Correos eliminados del servidor**
☐ **Remitente bloqueado**
☐ **Contraseñas cambiadas**

☐ **Sesiones activas cerradas**
☐ **Archivo puesto en cuarentena**
☐ **Sistema apagado**
☐ **Evidencia recolectada**

Otras acciones:

Contención efectiva: ☐ Sí ☐ No ☐ Parcial

SECCIÓN 7: CRONOLOGÍA DE EVENTOS

Fecha/Hora	Evento	Responsable
	Inicio estimado del incidente	
	Primera detección	
	Notificación al equipo de seguridad	
	Inicio de contención	

SECCIÓN 8: ANÁLISIS Y CAUSA RAÍZ

Vector de ataque:
☐ **Correo electrónico (phishing)**
☐ **Navegación web (drive-by download)**
☐ **Vulnerabilidad explotada**
☐ **Credenciales comprometidas**
☐ **Medios removibles (USB)**
☐ **Software vulnerable**
☐ **Ingeniería social**

☐ **Desconocido**
☐ **Otro: _____**

Causa raíz identificada:

_____
_____
_____

Controles que fallaron:

_____
_____
_____

SECCIÓN 9: REMEDIACIÓN

Acciones de erradicación:

☐ **Limpieza con antivirus**
☐ **Reimagen de sistema(s)**
☐ **Reinstalación de aplicaciones**
☐ **Remoción manual de persistencia**
☐ **Actualización de sistemas**
☐ **Parcheado de vulnerabilidades**

Detalles:

_____
_____

Sistemas restaurados: ☐ Sí ☐ No ☐ En proceso

Fecha/Hora de restauración: //_____ :

_____

SECCIÓN 10: VALIDACIÓN Y CIERRE

Verificación post-remediación:

☐ **Escaneo completo sin detecciones**
☐ **No se observa actividad sospechosa**
☐ **Conexiones de red normales**

☐ **Usuarios pueden trabajar normalmente**
☐ **Monitoreo establecido (_____ días)**

Estado final:
☐ **RESUELTO - Sin actividad residual**
☐ **MITIGADO - Riesgo reducido, monitoreo continuo**
☐ **EN INVESTIGACIÓN - Requiere análisis adicional**

Fecha de cierre: //_____ :

SECCIÓN 11: COMUNICACIONES

Notificaciones realizadas:

Fecha/Hora	Persona/Área notificada	Medio	Asunto

Comunicación externa requerida:
☐ **No**
☐ **Sí - Proveedor de servicio**
☐ **Sí - Autoridades**
☐ **Sí - Usuarios afectados**
☐ **Sí - Otro: _____**

SECCIÓN 12: LECCIONES APRENDIDAS

¿Qué funcionó bien?

¿Qué se pudo hacer mejor?

Recomendaciones para prevenir recurrencia:

1. _____
2. _____
3. _____

Controles a implementar/mejorar:

☐ **Actualización de firmas de antivirus**
☐ **Nuevas reglas de firewall**
☐ **Alertas adicionales en Graylog**
☐ **Políticas de correo reforzadas**
☐ **Capacitación de usuarios**
☐ **Actualización de procedimientos**
☐ **Endurecimiento de sistemas**
☐ **Otro: _____**

SECCIÓN 13: INFORMACIÓN ADICIONAL

Costo estimado del incidente:

Concepto	Monto
Horas de personal	
Herramientas/servicios externos	
Datos/sistemas perdidos	
Total estimado	

Tiempo total de resolución: _____ horas/días

Archivos adjuntos:
☐ **Logs recolectados**
☐ **Capturas de pantalla**
☐ **Análisis de malware**
☐ **Evidencia forense**
☐ **Comunicaciones relacionadas**

Ubicación de evidencia: _____

APROBACIONES

Analista de Seguridad:
Nombre: _____ Fecha: //_____
Firma: _____

CISO:
Nombre: _____ Fecha: //_____
Firma: _____

Director de TI (si aplica para incidentes CRÍTICOS/ALTO):
Nombre: _____ Fecha: //_____
Firma: _____

NOTAS ADICIONALES

Revisiones posteriores:

Fecha	Revisado por	Cambios
