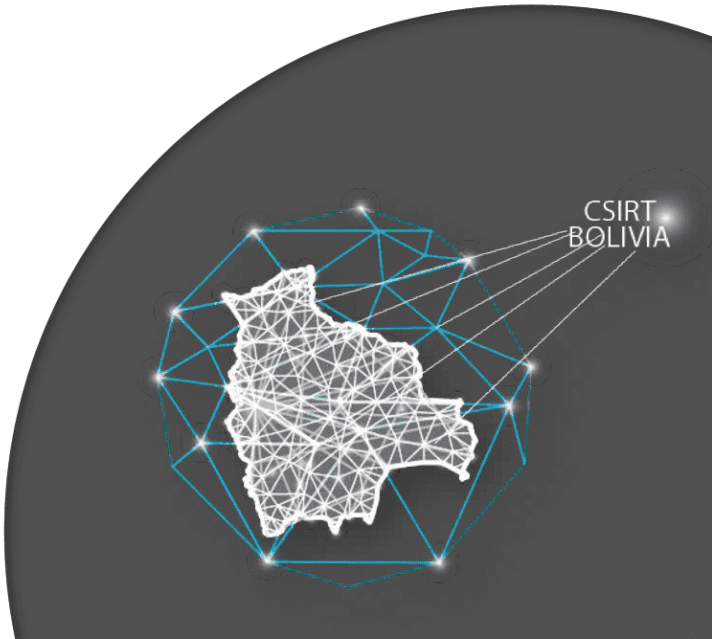
ESTADO PLURINACIONAL DE BOLIVIA
MINISTERIO DE LA PRESIDENCIA

AGETIC
Digitalizando Bolivia
Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación

INFORME DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES



ENERO - FEBRERO 2021

Índice

Índice de tablas

Índice de gráficos

1. Resumen Ejecutivo

El Centro de Gestión de Incidentes Informáticos (CGII) de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) presenta el informe de gestión de incidentes y vulnerabilidades correspondiente a enero y febrero de 2021 en el marco del Decreto Supremo 2514 que establece las funciones del CGII.

- Monitorear los sitios web gubernamentales y la aplicación de las políticas y lineamientos definidos por la AGETIC.
- Comunicar y otorgar información a todas las entidades del sector público acerca de incidentes informáticos y vulnerabilidades de los que se haya tomado conocimiento.
- Prestar soporte técnico a las entidades del sector público en caso de que ocurriese un incidente informático.
- Otorgar soporte técnico para la prevención de incidentes informáticos a las entidades del nivel central del Estado a solicitud de las mismas.
- Coordinar la gestión de incidentes informáticos gubernamentales con entidades de similar función a nivel internacional.

Durante este mes se gestionaron 80 tickets de incidentes y vulnerabilidades que corresponden a reportes nuevos y abiertos de meses anteriores. Del total de tickets, 37, fueron resueltos a través de la correcta comunicación, seguimiento y validación con las entidades afectadas; 43 tickets se encuentran abiertos y están siendo gestionados para solucionarlos, cuyos resultados serán reflejados en el siguiente informe.

El presente informe muestra estadísticas de la atención de tickets válidos de incidentes y vulnerabilidades durante los meses de enero y febrero, cuyos datos son clasificados por casos “tipo” en términos de cantidad y porcentaje.

También se hace una relación porcentual entre los tickets que fueron resueltos en el transcurso del mes y de aquellos que están en proceso de resolución.

2. Alcances

La información de cantidades y porcentajes mostrados en el presente informe corresponden a tickets gestionados por el CGII de enero a febrero, a partir de reportes válidos de incidentes y vulnerabilidades realizados por las siguientes fuentes:

- Responsables de Seguridad de la Información de las entidades del sector público.
- Herramientas de monitoreo y detección implementadas por el CGII.
- Equipos de Respuesta ante Incidentes Informáticos.
- Participantes del muro de la fama a través del formulario de reporte.

3. Actividades

A continuación las actividades realizadas por el CGII durante el referido período de tiempo:

- Análisis de indicadores de compromiso obtenidos de fuentes abiertas de información que tienen incidencia en entidades del sector público.
- Validación de reportes para descartar falsos positivos que no corresponden.

- Creación de tickets para comunicar el incidente o vulnerabilidad a la entidad afectada, brindando la información técnica necesaria para su solución.
- Seguimiento al estado de solución de los casos pendientes a través de llamadas telefónicas y correo electrónico, también soporte técnico en caso que así lo requieran.
- Validación de las medidas aplicadas por la entidad para solucionar el incidente o vulnerabilidad, y posterior cierre del ticket.
- Monitoreo de disponibilidad de 548 sitios web pertenecientes a entidades del sector público.
- Detección de incidentes y vulnerabilidades.

4. Estadísticas

Las siguientes estadísticas presentadas en tablas y gráficos corresponden a tickets abiertos y resueltos de reportes de incidentes y vulnerabilidades gestionadas durante los meses de enero y febrero.

4.1. Tickets abiertos

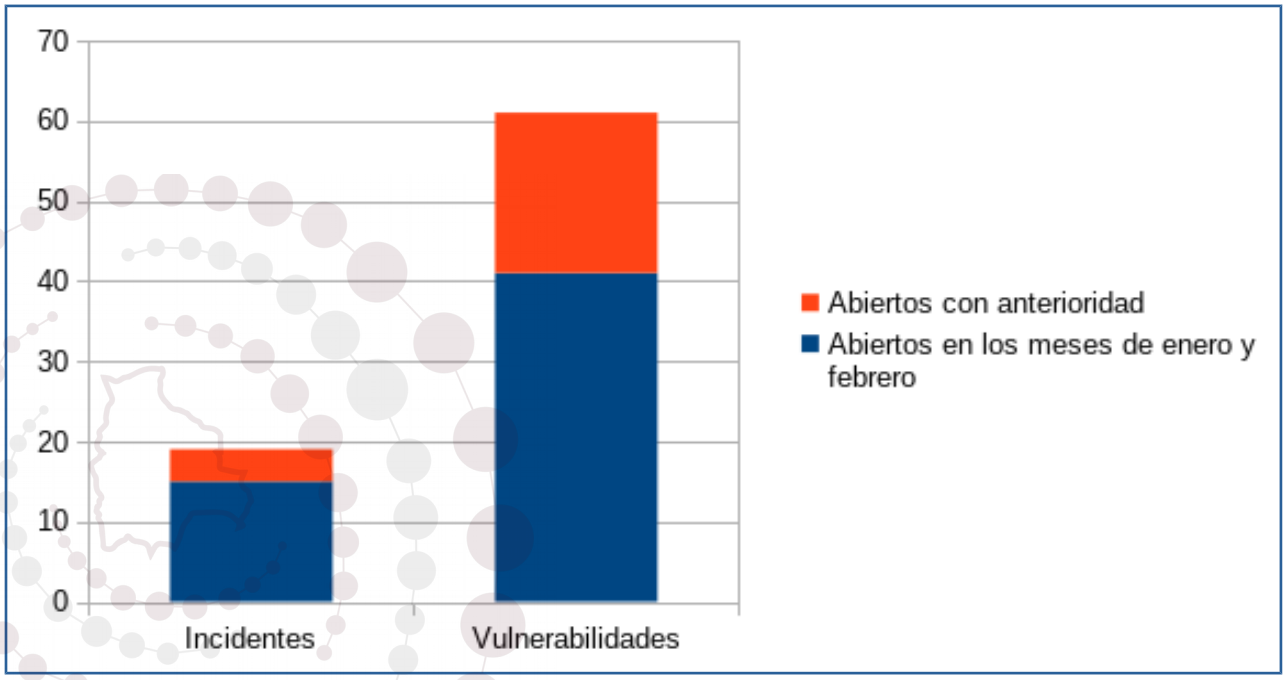
En los meses de enero y febrero, se gestionaron 80 tickets, los cuales representan casos de incidentes y vulnerabilidades, 56 fueron abiertos en enero-febrero y 24 corresponden a meses anteriores; en la siguiente tabla se podrá apreciar la información desagregada:

Tabla 1: Detalle de tickets abiertos

Tipo	Tickets	Cantidad
Vulnerabilidades	Abiertos en enero y febrero	41
	Abiertos con anterioridad	20
Incidentes	Abiertos en enero y febrero	15
	Abiertos con anterioridad	4
Totales	**Tickets abiertos**	**80**

En el siguiente gráfico se puede observar la distribución porcentual de tickets abiertos de incidentes y vulnerabilidades en enero y febrero:

Gráfico 1: Tickets abiertos



4.2. Tickets abiertos por categoría

4.2.1 Incidentes

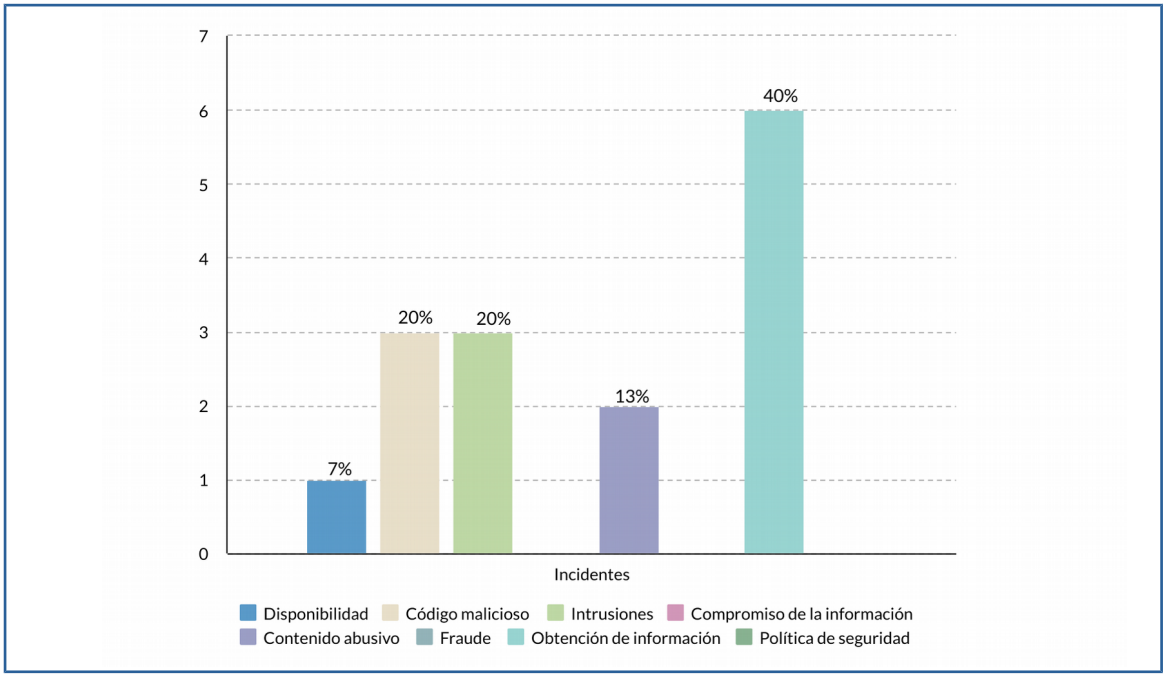
En enero y febrero se registraron 15 tickets nuevos de incidentes, que fueron categorizados de acuerdo al detalle representado por la siguiente tabla y su respectivo gráfico:

Tabla 2: Tickets de incidentes por categoría

Categoría	Tickets	Porcentaje
Código malicioso	3	20 %
Compromiso de la información	0	0 %
Contenido abusivo	2	13 %
Disponibilidad	1	7 %
Fraude	0	0 %
Intrusiones	3	20 %
Obtención de información	6	40 %
Política de seguridad	0	0 %
Totales	**15**	**100 %**

Dentro de las categorías:***obtención de información, código malicioso e intrusiones,*** que cuentan con la mayor cantidad de tickets, se gestionaron casos de phishing, spam distribuidos a través de correos electrónicos con la finalidad de obtener la contraseña de los usuarios, distribución de virus e intrusiones a sitios web.

Gráfico 2: Tickets de incidentes por categoría



4.2.2 Vulnerabilidades

Durante los meses de enero y febrero se registraron 41 tickets nuevos de vulnerabilidades, que han sido categorizados de acuerdo a detalle de la siguiente tabla y su gráfico:

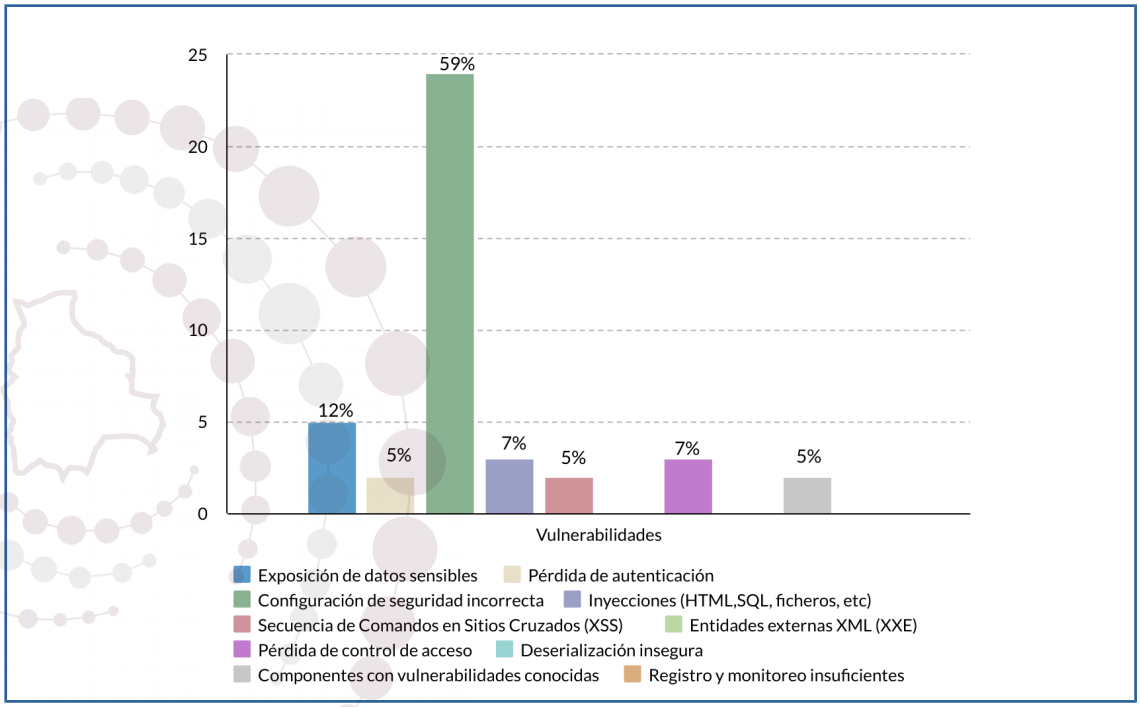
Tabla 3: Tickets de vulnerabilidades por categoría

Categoría	Tickets	Porcentaje
Exposición de datos sensibles	5	12 %
Pérdida de autenticación	2	5 %
Configuración de seguridad incorrecta	24	59 %
Inyecciones (HTML, SQL, ficheros)	3	7 %

Categoría	Tickets	Porcentaje
Secuencia de Comandos en Sitios Cruzados (XSS)	2	5 %
Entidades externas XML (XXE)	0	0 %
Pérdida de control de acceso	3	7 %
Deserialización insegura	0	0 %
Componentes con vulnerabilidades conocidas	2	5 %
Registro y monitoreo insuficientes	0	0 %
Totales	**41**	**100%**

Como se aprecia en la gráfica, la vulnerabilidad de ***Configuración de seguridad incorrecta***, predominó durante los meses de enero y febrero seguido de la ***Exposición de datos sensibles*** presentes en sistemas de información de entidades del sector público.

Gráfico 3: Tickets de vulnerabilidades por categoría



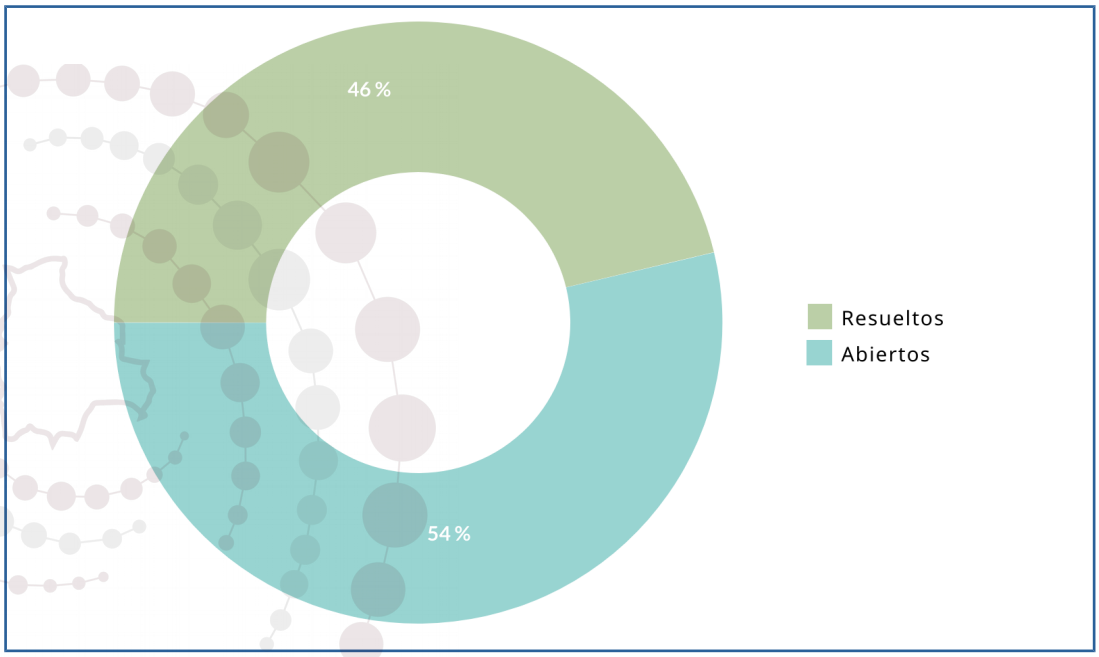
4.3. Tickets resueltos

Como resultado de las actividades de gestión de incidentes y vulnerabilidades en enero y febrero, el CGII resolvió 37 tickets, motivo por el cual quedan pendientes de solución para el siguiente mes 43 tickets, a los cuales se está dando el seguimiento respectivo. Estos datos se aprecian en la siguiente tabla y su correspondiente gráfico:

Tabla 4: Tickets abiertos y resueltos

Estado	Tickets	Porcentaje
Resueltos	37	46 %
Abiertos (En curso)	43	54 %
Totales	**80**	**100%**

Gráfico 4: Porcentaje de tickets resueltos



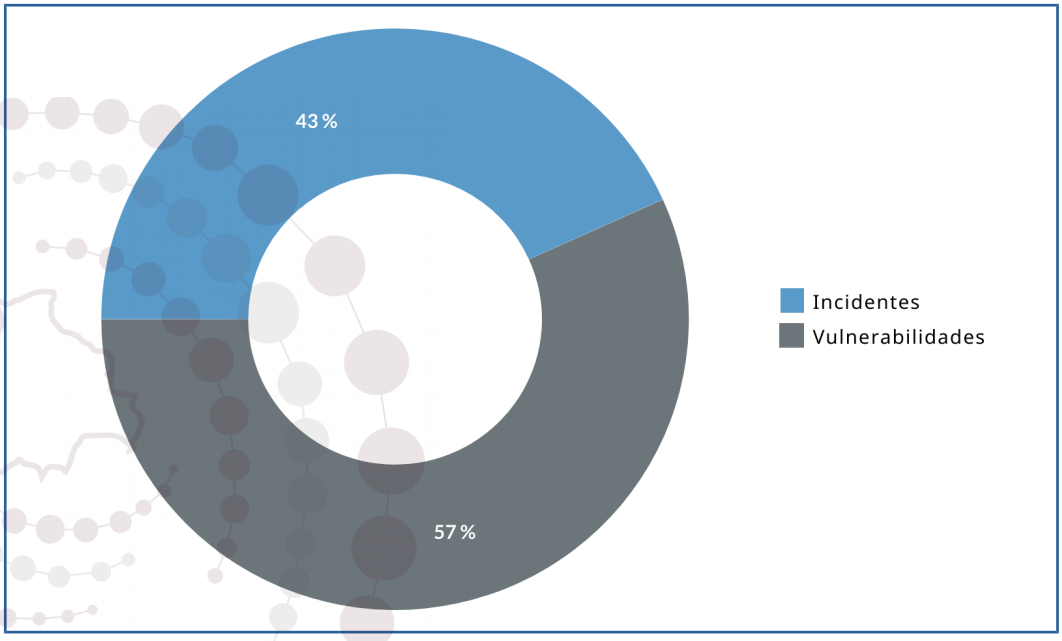
4.4. Tickets resueltos por vulnerabilidad e incidente

Del total de tickets resueltos en los meses de enero y febrero, 16 corresponden a incidentes y 21 a vulnerabilidades, datos que se pueden observar en la siguiente tabla y su correspondiente gráfico:

Tabla 5: Tickets resueltos por vulnerabilidad e incidente

Tipo	Tickets	Porcentaje
Incidentes	16	43 %
Vulnerabilidades	21	57 %
Totales	**37**	**100%**

Gráfico 5: Tickets resueltos



5. Términos y definiciones

Código malicioso.- Programas informáticos que tienen como objetivo acceder al sistema sin ser detectados y realizar acciones como el secuestro de información o recopilación de datos privados.

Componentes con vulnerabilidades conocidas.- Los componentes como bibliotecas, frameworks y otros módulos se ejecutan con los mismos privilegios que la aplicación; si se explota un componente vulnerable, el ataque puede provocar pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas que pueden debilitar las defensas y permitir diversos ataques e impactos.

Compromiso de la información.- Acceso, modificación, borrado o publicación de información sin autorización del propietario.

Configuración de seguridad incorrecta.- Una configuración errónea de seguridad surge cuando dichas configuraciones se definen, implementan y se mantienen con valores predeterminados.

Contenido abusivo.- Incidentes que muestren signos evidentes de correos electrónicos no solicitados.

Deserialización insegura.- Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos que pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor.

Disponibilidad.- Falta de disponibilidad del sistema o servicio producto de ataques de denegación de servicio, mala configuración, interrupciones de servicio por factores no previstos.

Entidades externas XML (XXE).- Muchos procesadores XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Un ataque de entidad externa XML exitoso puede revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS).

Exposición de datos sensibles.- Acceso a datos sensibles como contraseñas, claves privadas de API, errores o debug, rutas completas, datos personales o uso de algoritmos de cifrado débil.

Fraude.- Incidentes que tengan nexo con el uso no autorizado, derechos de autor, suplantación de identidad, exfiltración de información o uso ilegítimo de credenciales.

Incidente.- Evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Intrusiones.- Acceso al sistema o a uno de sus componentes aprovechando sus vulnerabilidades.

Inyecciones.- Son fallas de inyección, como SQL, NoSQL, OS o LDAP que ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta.

Obtención de información.- Obtención de datos personales, información de las redes de datos, credenciales de acceso del usuario a través de técnicas de engaño.

Pérdida de Autenticación.- Este tipo de debilidad puede permitir a un atacante capturar u omitir los métodos de autenticación que usa una aplicación web.

Pérdida de control de acceso.- Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos.

Política de seguridad.- Incidentes de abuso de privilegios de los usuarios, acceso a servicios no autorizados, o relacionados al uso de sistemas desactualizados.

Registro y monitoreo insuficientes.- El registro y monitoreo insuficiente, junto a la falta de respuesta ante incidentes permite a los atacantes mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos. Historial de cambios

Secuencia de Comandos en Sitios Cruzados (XSS).- Los XSS ocurren cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada; o actualiza una página web existente con datos suministrados por el usuario utilizando una API que ejecuta JavaScript en el navegador.

Ticket abierto.- Reporte de un incidente o vulnerabilidad que fue validado y se encuentra en proceso de resolución.

Ticket resuelto.- Reporte de un incidente o vulnerabilidad que fue resuelta satisfactoriamente.

Vulnerabilidad.- Debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la misma, pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad.

6. Historial de cambios

Versión	Fecha	Autor	Descripción	Motivo de cambios
1.0	02/03/2021	Gonzalo Vargas	Elaboración	Datos iniciales, estructura y datos
1.0	10/03/2021	Victor Jimenez	Revisión	Redacción, línea gráfica
1.0	10/03/2021	Franz Rojas	Aprobación	Aprobación