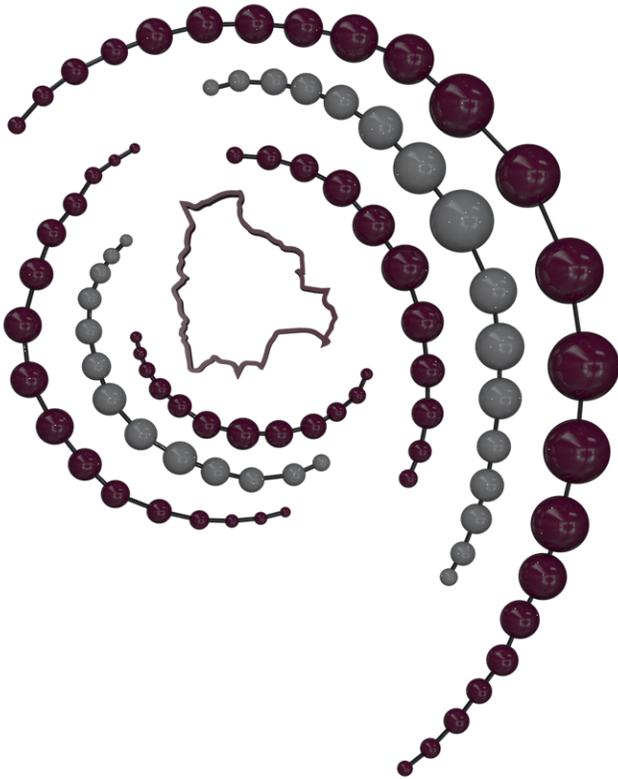




ESTADO PLURINACIONAL DE
BOLIVIA MINISTERIO DE
LA PRESIDENCIA

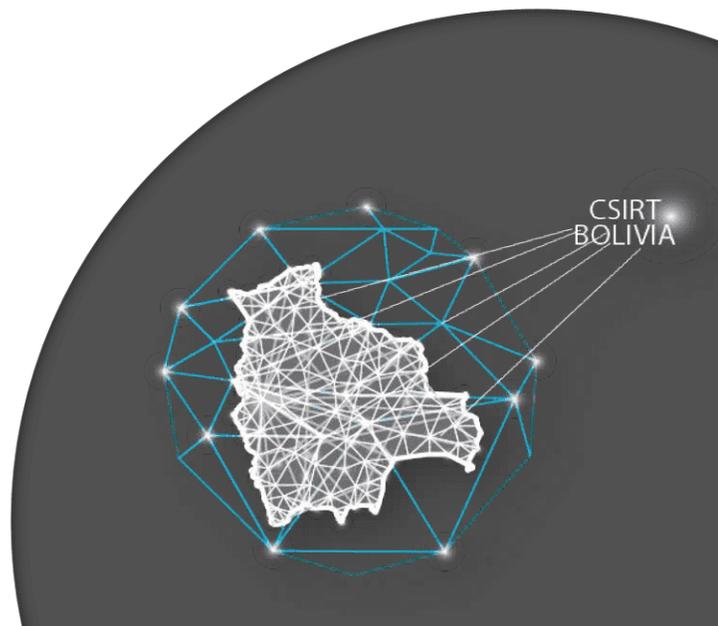


AGETIC | Agencia de Gobierno Electrónico y
Digitalizando Bolivia | Tecnologías de Información y Comunicación



INFORME DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES

**GESTIÓN
2020**



Índice

1. Resumen Ejecutivo.....	3
2. Alcances.....	4
3. Actividades.....	4
4. Estadísticas.....	5
4.1. Tickets abiertos.....	5
4.2. Tickets abiertos por categoría.....	7
4.2.1 Incidentes.....	7
4.2.2 Vulnerabilidades.....	8
4.3. Tickets resueltos.....	10
4.4. Tickets resueltos por vulnerabilidad e incidente.....	11
5. Términos y definiciones.....	12
6. Historial de cambios.....	16

Índice de tablas

Tabla 1: Detalle de tickets abiertos.....	6
Tabla 2: Tickets de incidentes por categoría.....	7
Tabla 3: Tickets de vulnerabilidades por categoría.....	8
Tabla 4: Tickets abiertos y resueltos.....	10
Tabla 5: Tickets resueltos por vulnerabilidad e incidente.....	11

Índice de gráficos

Gráfico 1: Tickets abiertos.....	6
Gráfico 2: Tickets de incidentes por categoría.....	8
Gráfico 3: Tickets de vulnerabilidades por categoría.....	9
Gráfico 4: Porcentaje de tickets resueltos.....	10
Gráfico 5: Tickets resueltos.....	11

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 la gestión 2020 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 el año 2020 se gestionaron 624 tickets de incidentes y vulnerabilidades. Del total de tickets, 600 fueron resueltos a través de la correcta comunicación, seguimiento y validación con las entidades afectadas; 24 tickets están siendo gestionados para solucionarlos, cuyos resultados se reflejarán en la gestión 2021.

El presente informe muestra estadísticas de la atención de tickets válidos de incidentes y vulnerabilidades durante la gestión 2020, 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 año 2020 y de aquellos que están en proceso de solución.

2. Alcances

La información de cantidades y porcentajes mostrados en el presente informe corresponden a tickets gestionados por el CGII durante el año 2020, 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 ser atendidos.
- 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, otorgando soporte técnico en caso de ser requerido.
- 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 el año 2020.

4.1. Tickets abiertos

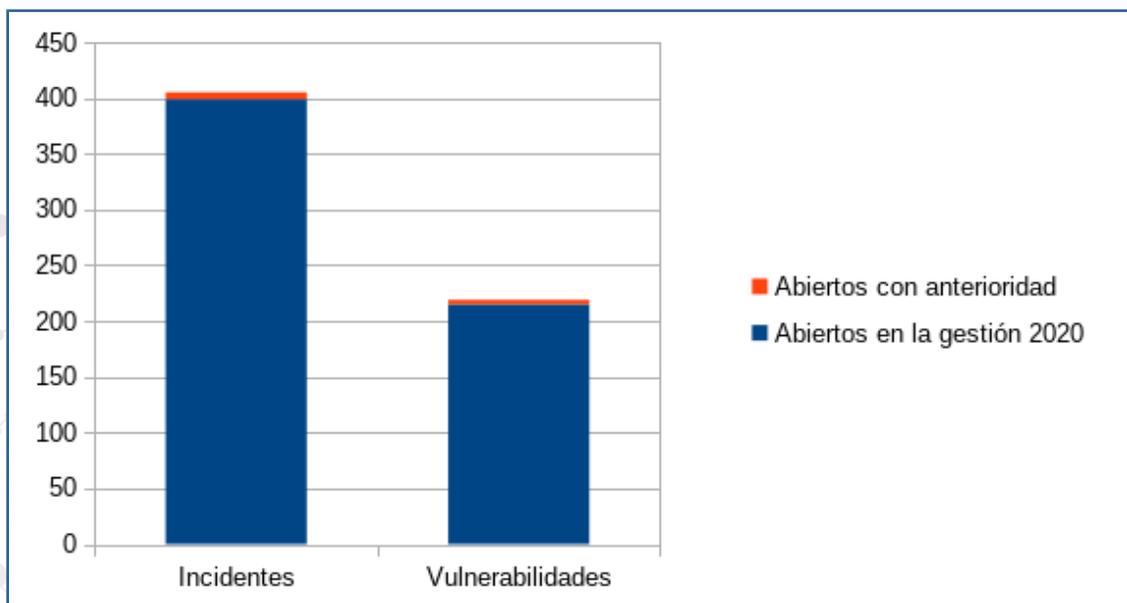
Durante el año 2020, se gestionaron 624 tickets, los cuales representan casos de incidentes y vulnerabilidades, 614 fueron abiertos en el año 2020 y 10 corresponden a la gestión anterior; en la siguiente tabla se podrá apreciar la información desagregada:

Tabla 1: Detalle de tickets abiertos

Tipo	Tickets	Cantidad
Vulnerabilidades	Abiertos en la gestión 2020	215
	Abiertos en periodos anteriores	4
Incidentes	Abiertos en la gestión 2020	399
	Abiertos en periodos anteriores	6
Totales	Tickets abiertos	624

En el siguiente gráfico se puede observar la distribución porcentual de tickets abiertos de incidentes y vulnerabilidades en la gestión 2020:

Gráfico 1: Tickets abiertos



4.2. Tickets abiertos por categoría

4.2.1 Incidentes

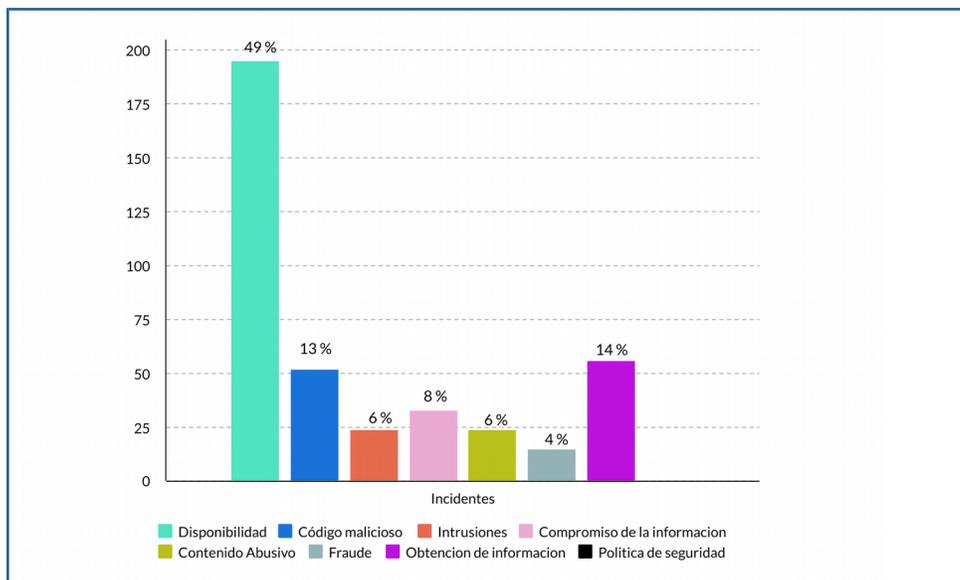
En la gestión 2020 se registraron 399 tickets nuevos de incidentes, que han sido categorizados de acuerdo al detalle representado por la siguiente tabla y su respectivo gráfico:

Tabla 2: Tickets de incidentes por categoría

Categoría	Tickets	Porcentaje
Disponibilidad	195	49 %
Código malicioso	52	13 %
Intrusiones	24	6 %
Compromiso de la información	33	8 %
Contenido abusivo	24	6 %
Fraude	15	4 %
Obtención de información	56	14 %
Política de seguridad	0	0 %
Totales	399	100 %

Dentro de la categoría **disponibilidad** que cuentan con la mayor cantidad de tickets, se tuvieron incidentes relacionados a fallas de hardware, software y denegación de servicio, en **obtención de información** se presentaron casos de phishing a través de correo electrónico, y en la categoría **código malicioso**, incidentes de ransomware, virus y troyanos.

Gráfico 2: Tickets de incidentes por categoría



4.2.2 Vulnerabilidades

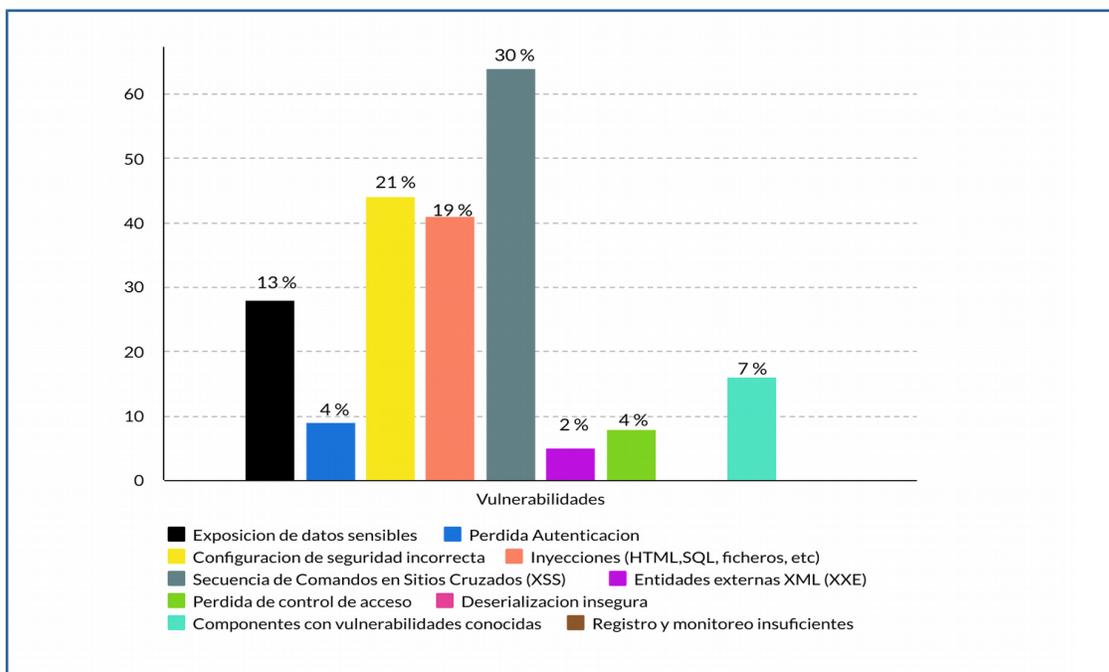
Durante la gestión 2020 se registraron 215 tickets de vulnerabilidades, que han sido categorizados de acuerdo a detalle de la siguiente tabla y su gráfico:

Tabla 3: Tickets de vulnerabilidades por categoría

Categoría	Tickets	Porcentaje
Exposición de datos sensibles	28	13 %
Pérdida de autenticación	9	4 %
Configuración de seguridad incorrecta	44	21 %
Inyecciones (HTML, SQL, ficheros)	41	19 %
Secuencia de Comandos en Sitios Cruzados (XSS)	64	30 %
Entidades externas XML (XXE)	5	2 %
Pérdida de control de acceso	8	4 %

Categoría	Tickets	Porcentaje
Deserialización insegura	0	0 %
Componentes con vulnerabilidades conocidas	16	7 %
Registro y monitoreo insuficientes	0	0 %
Totales	215	100%

Gráfico 3: Tickets de vulnerabilidades por categoría



Como se aprecia en la gráfica, la vulnerabilidad de **Secuencia de comandos en sitios cruzados**, predominó durante la gestión 2020 seguido de la **Configuración de seguridad incorrecta** presentes en sistemas de información de entidades del sector público.

4.3. Tickets resueltos

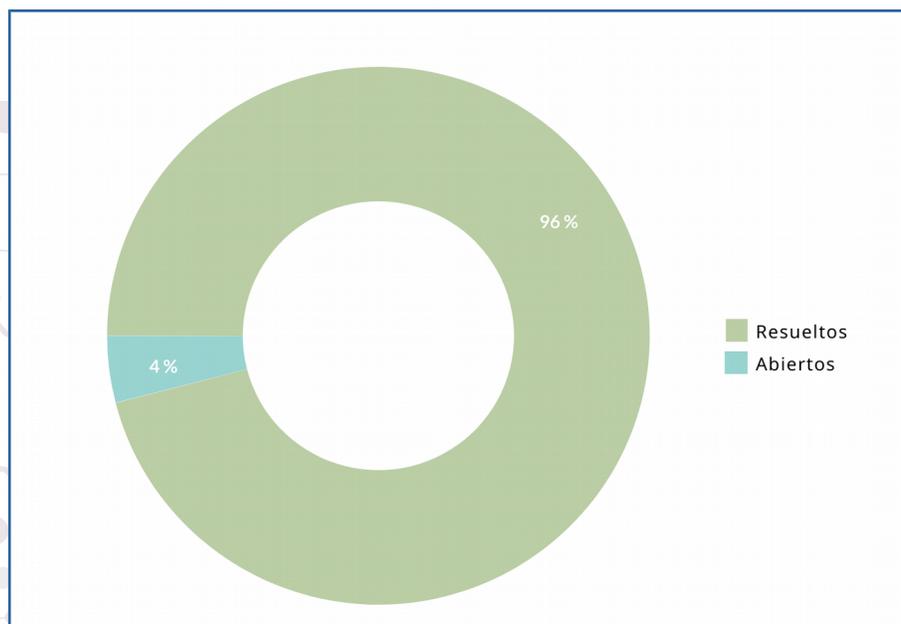
Como resultado de las actividades de gestión de incidentes y vulnerabilidades en el año 2020, el CGII resolvió 600 tickets, quedando pendientes de solución para la presente gestión 24 tickets, a los cuales se está dando el seguimiento respectivo para su solución y posterior cierre.

Estos datos se aprecian en la siguiente tabla y su gráfico:

Tabla 4: Tickets abiertos y resueltos

Estado	Tickets	Porcentaje
Resueltos	600	96 %
Abiertos (En curso)	24	4 %
Totales	624	100%

Gráfico 4: Porcentaje de tickets resueltos



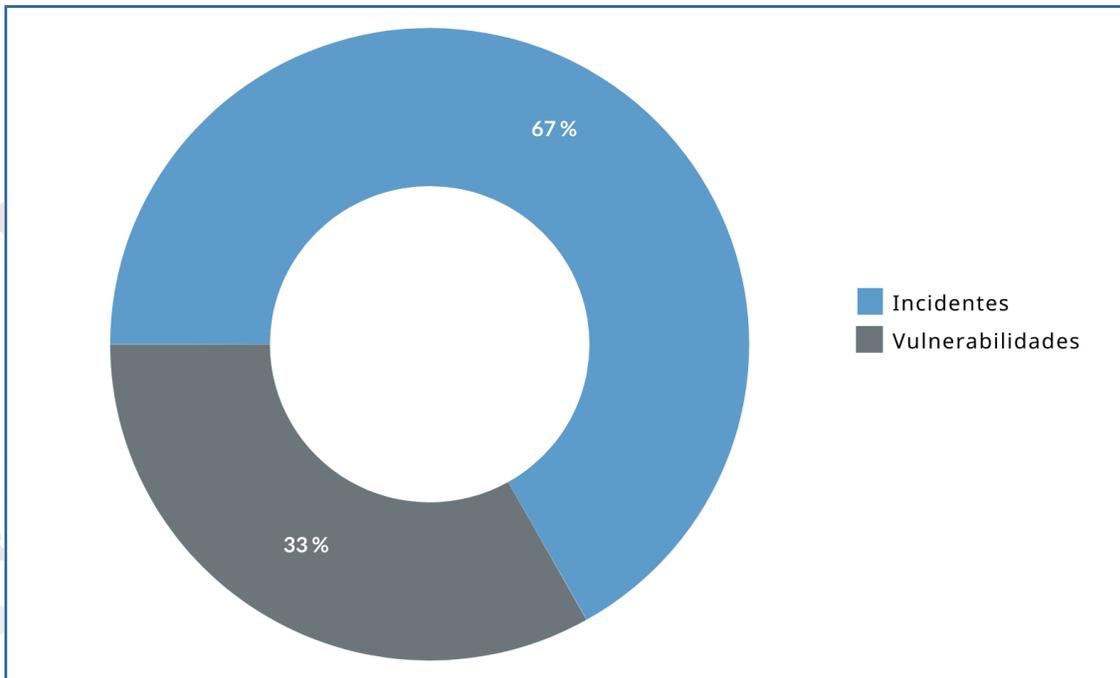
4.4. Tickets resueltos por vulnerabilidad e incidente

Del total de tickets resueltos en la gestión 2020, 401 corresponden a incidentes y 199 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	401	67 %
Vulnerabilidades	199	33 %
Totales	600	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	Krissia Ferreira	Elaboración	Datos iniciales, estructura y datos
1.0	09/03/2021	Víctor Jimenez	Revisión	Redacción, línea gráfica
1.0	10/03/2021	Franz Rojas	Aprobación	Aprobación

