ATENCIÓN DE EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por:	Revisado por:	Aprobado por:
Grover Omar Sotelo López Oficial de Seguridad Digital	Kelly Elizabeth Paz Orellana Jefa (e) de la Unidad de Modernización	Marco Antonio Mena Miranda Jefe de la Oficina de Tecnologías de Información

CONTROL DE CAMBIOS

N°	Ítems (Sección del documento)	Descripción del cambio
1	-	• Versión inicial del documento

ÍNDICE

1. OBJETIVO

Establecer las instrucciones para la atención de eventos o debilidades de seguridad de la información reportados por el personal de la Sunass y terceros a fin de asegurar una rápida y efectiva respuesta.

2. ALCANCE

El presente documento es aplicable a todo el personal de la OTI que se le asigne la atención de un evento o debilidad de seguridad de la información reportados por el SMA y al Oficial de Seguridad Digital.

3. DEFINICIONES

3.1 **Activo de información:** Es cualquier elemento que tenga valor para la organización y, en consecuencia, debe ser protegido.

3.2 **Amenaza:** Factor externo o interno que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la organización. No existe una única clasificación de las amenazas, lo importante es considerarlas todas a la hora de su identificación.

3.3 **Evento de Seguridad de la Información:** Ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación a la política de seguridad de la información o falla de controles, o una situación previamente desconocida que pueda ser relevante para la seguridad.

3.4 **Debilidad de Seguridad de la Información:** Vulnerabilidades en los controles de seguridad de la información implementados, las cuales pueden ser aprovechadas para evadir los controles y podrían provocar un evento y/o incidente de seguridad de la información.

3.5 **Impacto:** Consecuencias que produce un incidente de seguridad sobre la organización.

3.6 **Incidente de Seguridad de la Información:** Evento o serie de eventos de seguridad de la información, no deseados o inesperados, que tienen una significativa probabilidad de comprometer las operaciones y amenazan la seguridad de la información.

3.7 **Sistema de Mesa de Ayuda**: Sistema de información en el que un usuario registra los eventos o debilidades que identifica.

4. SIGLAS / ACRONIMOS

SMA : Sistema de Mesa de Ayuda
OTI : Oficina de Tecnologías de Información

5. DISPOSICIONES GENERALES

5.1 El monitoreo permanente debe prever los incidentes de seguridad de la información, logrando identificar e implementar controles preventivos y correctivos que aseguren la información de la organización.

5.2 El personal responsable del SMA, debe revisar los eventos o debilidades reportados al SMA para identificar si están relacionados a seguridad de la información y comunicarlos al Oficial de Seguridad Digital para su revisión.

6. DESCRIPCIÓN DEL INSTRUCTIVO

6.1 Registro de eventos y debilidades en la Bitácora de Seguridad de la Información

a) Registro de debilidades

El Oficial de Seguridad Digital registra la debilidad reportada en el formato "Bitácora de Gestión de Eventos y Debilidades de Seguridad de la Información" para las gestiones respectivas. La información que se debe registrar como mínimo es la siguiente:

- Descripción de la Debilidad reportada.
- Fecha en la que se reportó.
- Número de ticket generado por el SMA.
- Datos del usuario que reporto la debilidad.
- Comentarios.

El Oficial de Seguridad Digital determina si la debilidad identificada requiere ejecutar alguna acción y establece un plan de acción; caso contrario:

- Si de la revisión se identifica que no corresponde aplicar ninguna acción para el tratamiento de la debilidad reportada, sólo se mantiene el registro en la bitácora.
- Si se identifica que la debilidad reportada no corresponde a uno de los tipos indicados en la **Tabla N° 1 "Tipos de Debilidades de Seguridad de la Información"** del Anexo N° 1, esta se devuelve al responsable del SMA.

b) Registro de eventos

El responsable del SMA identifica que tipo de evento de seguridad de la información fue reportado de acuerdo con la **Tabla N° 2 "Tipos de Eventos de Seguridad de la Información"** del Anexo N° 1 y deriva al Oficial de Seguridad Digital mediante el SMA para la evaluación respectiva.

El Oficial de Seguridad Digital registra el evento reportado en el formato "Bitácora de Gestión de Eventos y Debilidades de Seguridad de la Información" para las gestiones respectivas. La información que se debe registrar como mínimo es la siguiente:

- Descripción del Evento reportado.
- Fecha en la que se reportó.
- Número de ticket generado por el SMA.
- Datos del usuario que reporto el evento.
- Tipo de Evento, según la Tabla N° 1 del Anexo.
- Comentarios.

6.2 Evaluación de eventos de seguridad de la información

a) El Oficial de Seguridad Digital evalúa el evento de seguridad de la información de acuerdo con las condiciones que se describen en la tabla **"Niveles de Impacto de Eventos de Seguridad de la Información"** del Anexo N° 2, para determinar el nivel de impacto del evento reportado.

b) Se debe considerar que todos los eventos que se determinen con un nivel de impacto "Medio" y "Alto" se convierten en Incidentes de Seguridad de la Información.

c) El Oficial de Seguridad Digital de acuerdo con su evaluación determina el nivel de escalamiento para el adecuado tratamiento de los incidentes según la tabla **"Niveles de Escalamiento de Eventos/ Incidentes de Seguridad de la Información"** del Anexo N° 3.

d) El Oficial de Seguridad Digital debe evaluar todos los eventos de seguridad de la información con "bajo nivel de impacto" para determinar cuáles de estos requieren una alternativa de solución temporal.

6.3 Tratamiento de los incidentes de seguridad de la información

a) Comunicación del incidente

El Oficial de Seguridad Digital comunica el incidente a los responsables de darle solución, a los propietarios de los activos de información afectados y a otros usuarios según se considere necesario, por correo electrónico.

b) Solución temporal del Incidente

Al haber encontrado una posible solución al incidente, se verifica que los activos afectados vuelvan a su condición operativa y se registra en el formato "Bitácora de Gestión de Eventos y Debilidades de Seguridad de la Información", considerando lo siguiente:

- Cuando se trate de incidentes de seguridad de la información tecnológicos se deriva al personal de la OTI para su atención.
- Cuando se trate de incidentes de seguridad de la información no tecnológicos se deriva al propietario del activo de información afectado.

c) Recolección de Evidencias

Se establece una cadena de custodia y no se elimina ningún registro hasta que el incidente se haya cerrado. Para tal fin se debe:

- Analizar el incidente.
- Buscar la información.
- Preservar la evidencia.

En el caso que la Sunass determine que las evidencias deben tener un método especial de recolección para que sean utilizadas con fines legales o sancionadores, se debe de tener en consideración lo establecido en el Anexo 4 **"Pautas para la Recolección de Evidencias"**.

d) Análisis de causa

El Oficial de Seguridad Digital o a quien corresponda identifica las causas que originan el incidente de seguridad de la información. El resultado del análisis debe ser registrado por el Oficial de Seguridad Digital en la "Bitácora de Gestión de Eventos y Debilidades de Seguridad de la Información".

e) Escalamiento del incidente

Cuando el incidente de seguridad de la información no pueda ser resuelto internamente, el Oficial de Seguridad Digital debe escalarlo a las autoridades externas competentes (contactos de cooperación o asesores externos) en seguridad de la información si las consecuencias del incidente lo ameritan, de acuerdo con lo indicado en la tabla **"Niveles de Escalamiento de Eventos/ Incidentes de Seguridad de la Información"** del Anexo N° 3.

f) Registrar las acciones tomadas

El Oficial de Seguridad Digital debe registrar las acciones ejecutadas en la "Bitácora de Gestión de Eventos y Debilidades de Seguridad de la Información", que ya son establecidas en la entidad para controlar el impacto ocasionado por el incidente de seguridad de la Información.

g) Retroalimentación al usuario

Una vez que el incidente haya sido solucionado y cerrado, el Oficial de Seguridad Digital comunica los resultados al usuario que reportó el incidente y a los afectados por el mismo, cierra el ticket en el SMA y se notifica de forma automática al usuario.

La documentación de la solución de los incidentes debe ser administrada por el Oficial de Seguridad Digital y ser registrada como lección aprendida en la "Bitácora de Gestión de Eventos y Debilidades de Seguridad de la Información", la cual será usada como retroalimentación para la implementación de mejoras en la atención de incidentes de seguridad de la información.

h) Histórico de Incidentes

El Oficial de Seguridad Digital debe mantener actualizada la "Bitácora de Gestión de Eventos y Debilidades de Seguridad de la Información", con la información obtenida para la solución de cada incidente.

5. ANEXOS

- Anexo N° 1: Tipos de eventos y debilidades de seguridad de la información.
- Anexo N° 2: Niveles de impacto de eventos de seguridad de la información.
- Anexo N° 3: Niveles de escalamiento de eventos / incidentes de seguridad de la información.
- Anexo N° 4: Pautas para la recolección de evidencias

ANEXO N° 1 - TIPOS DE EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN

TABLA N° 1 - TIPOS DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN

N°	TIPOS
1	Ausencia de control de accesos a un sistema de información o a la red.
2	No se realiza el bloqueo automático de las pantallas.
3	Ausencia de antivirus o antivirus desactualizado
4	Restauración de respaldo no exitoso
5	Copias de seguridad no exitosas
6	No se aplican prácticas de seguridad en el desarrollo de las aplicaciones.
7	No se cumple con el procedimiento de control de accesos
8	La información no está clasificada y/o etiquetada
9	No se aprecia seguridad física en las instalaciones de procesamiento y/u oficinas

TABLA N° 2 - TIPOS DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

N°	TIPOS
1	Ataques por software de tipo malicioso (malware)
2	Cambios no controlados en los sistemas (software y hardware) y servicios
3	Correos fraudulentos (phishing) solicitando información del usuario
4	Detección de vulnerabilidades de la seguridad
5	Identificación de protocolos en el tráfico de la red que sobrecargan el servicio
6	Incumplimientos de políticas, normas y/o procedimientos sobre seguridad de la Información
7	Mal uso y abuso del correo electrónico
8	Pérdida de servicio de TI, equipos de cómputo o acceso a las instalaciones
9	Pérdida o fuga de información física y/o digital
10	Violaciones de acceso a los sistemas
11	Accesos no autorizados

ANEXO N° 2 - NIVELES DE IMPACTO DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

Nivel	Descripción
Alto	Interrumpe seriamente la operación, el evento puede tener velocidad significativa / rápida en su propagación y ocasionar daños de activos de información. Podría llegar a afectar más de un tipo de activo. • Amenaza la preservación de la integridad, confidencialidad o disponibilidad de la información. • Afecta el buen nombre de la entidad. • Pérdida o robo de información confidencial de la organización o de terceros. • Afecta infraestructura crítica para los procesos de la entidad. • Genera incumplimiento de normas legales o contratos.
Medio	Interrumpe en un periodo corto de tiempo los procesos generales, el evento compromete un activo crítico. • Compromete medianamente el buen nombre de la entidad. • Se ve afectada medianamente la integridad, confidencialidad o disponibilidad de la información.
Bajo	No interrumpe los procesos, el evento se detecta y se puede controlar fácilmente con recursos existentes en la entidad. • No afecta la integridad, confidencialidad o disponibilidad de la información. • Impacta un número mínimo de activos de información que no son críticos.

ANEXO N° 3 - NIVELES DE ESCALAMIENTO DE EVENTO/INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Relevancia	Escalamiento
Nivel 1	Se escala al Comité de Gobierno Digital, proveedores pertinentes y si es el caso a las autoridades externas competentes.
Nivel 2	Oficial de Seguridad Digital con el apoyo del equipo técnico especializado y/o el Comité de Gobierno Digital
Nivel 3	Oficial de Seguridad Digital con áreas involucradas.

ANEXO N° 4 - PAUTAS PARA LA RECOLECCION DE EVIDENCIAS

1. **Durante la recolección de evidencias**
   - Se debe capturar una imagen del sistema tan precisa como sea posible.
   - Se deben realizar notas detalladas, que incluyan la fecha y hora y si se utiliza horario local o UTC.
   - Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo.
   - En el caso de enfrentarse a un dilema entre recolección y análisis, se debe elegir primero recolección y después análisis.
   - Recoger la información según el orden de volatilidad (de mayor a menor).
   - Tener en cuenta que por cada dispositivo el recojo de información puede realizarse de distinta manera.

   a. Orden de volatilidad

   El orden de volatilidad hace referencia al período de tiempo en el que está accesible cierta información, por lo que, se debe recolectar en primer lugar aquella información que vaya a estar disponible durante el menor período de tiempo; es decir, aquella cuya volatilidad sea mayor. Por ello, en la siguiente lista se muestra información ordenada de mayor a menor volatilidad como referencia:
   - Registros y contenido del caché.
   - Tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del kernel, memoria.
   - Información temporal del sistema.
   - Disco duro
   - Logs del sistema.
   - Configuración física y topología de la red.
   - Documentos.

   b. Acciones que deben evitarse

   Existen acciones que se deben evitar para no invalidar el proceso de recolección de información ya que debe preservarse su integridad, con la finalidad de que los resultados obtenidos puedan ser utilizados en un juicio, en caso sea necesario. Debe evitarse:
   - Apagar el ordenador hasta que se haya recopilado toda la información.
   - Confiar en la información proporcionada por los programas del sistema, ya que pueden estar comprometidos. Se debe recopilar la información mediante programas desde un medio protegido.
   - Ejecutar programas que modifiquen la fecha y hora de acceso de todos los archivos del sistema.

   c. Consideraciones sobre la privacidad

   Es muy importante tener en cuenta las siguientes consideraciones o pautas relacionadas a la privacidad:
   - Se debe solicitar una autorización por escrito de quien corresponda para poder llevar a cabo la recolección de evidencias, en el caso que se trabaje con información confidencial o de vital importancia para la Sunass, o que la disponibilidad de los servicios se vea afectada.
   - No se debe tener acceso a información personal de los usuarios, sin que se amerite una adecuada justificación.
   - No se deben recopilar datos que no sean parte del incidente de seguridad reportado.

2. Pautas para el almacenamiento de la evidencia

a. Cadena de custodia

La cadena de custodia debe estar claramente documentada y debe detallarse en un informe como mínimo los siguientes puntos:

- Número del incidente
- Fecha de reporte del incidente
- Descripción del incidente
- ¿Dónde?, ¿cuándo? y ¿quién? descubrió y recolectó la evidencia.
- ¿Dónde?, ¿cuándo? y ¿quién? manejó la evidencia.
- ¿Quién ha custodiado la evidencia?, ¿cuánto tiempo? y ¿cómo se ha almacenado?
- En el caso de que la evidencia cambie de custodio, indicar cuándo y cómo se realizó el intercambio.

b. Dónde y cómo almacenarlo

Se debe almacenar la información en dispositivos cuya seguridad haya sido demostrada y que permitan detectar intentos de acceso no autorizados.