INDICE:

Modificaciones respeto a la edición anterior:

1-Objetivo

Gestionar adecuadamente los incidentes y eventos de seguridad de la información, mediante el reporte oportuno de los usuarios, y el análisis de la información para reducir la afectación negativa de la seguridad de la información y/o la continuidad de las operaciones de VIDA.

2- Alcance

Inicia con la detección del incidente de seguridad de la información continua con la estrategia de contención y termina con el análisis post-incidente.

3. Referencias

- Norma ISO 27001

4.- Definiciones y abreviaturas

- **Activo de información**: Es cualquier elemento que tenga valor para la organización y, en consecuencia, debe ser protegido.
- **Amenaza**: Factor externo 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.
- **Autenticidad**: Aseguramiento de la organización respecto al origen cierto de los datos o información que circula por la Red.
- **Aviso de IDS sobre Buffer overflow**: Es un error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada.
- **Cadena de Custodia**: Registro detallado del tratamiento de la evidencia, incluyendo quienes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma
- **Contención**: Evitar que el incidente siga ocasionando daños.
- **Erradicación**: Eliminar la causa del incidente y todo rastro de los daños.
- **Evento de seguridad**: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
- **Gestión de Incidentes**: Es el conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder de manera eficaz y eficiente a incidentes de seguridad que afecten activos de una Organización. Minimizando su impacto en el negocio y la probabilidad que se repita.
- **Hash**: Función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija.
- **IDS**: Software de detección de intrusos
- **Impacto**: Consecuencias que produce un incidente de seguridad sobre la organización.
- **Incidente de seguridad de la información**: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Logs**: Registro de los sistemas de información que permite verificar las tareas o actividades realizadas por determinado usuario o sistema.
- **Recuperación**: Volver el entorno afectado a su estado natural.
- **Sniffers**: Software que captura los paquetes que viajan por la red para obtener información de la red o del usuario.
- **SSI**: Subsistema de Seguridad de la Información.
- **Validación**: Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.
- **Vulnerabilidad**: Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos y/o físicos.

5.- Realización

5.1- Responsabilidades

- Oficial de Seguridad de la Información:

Orientar y dar adecuado tratamiento a los incidentes de seguridad de la información detectados o reportados. Debe hacer un seguimiento periódico a los incidentes de seguridad presentados.

En caso de no presentarse un número significativo de reportes de incidentes de seguridad revisara los reportes de las herramientas de seguridad para el análisis pertinente y otras fuentes con el propósito de mejorar la gestión de incidentes de seguridad.

Debe mantener contactos apropiados con las autoridades, grupos de interés o foros externos que manejen las cuestiones relacionadas con incidentes de seguridad de la información.

- Funcionarios y contratistas

Deben tomar conciencia de su responsabilidad de reportar eventos y debilidades de seguridad de la información tan pronto como sea posible a la mesa de servicios internos.

Recibir las capacitaciones y participar en las campañas de sensibilización que se realicen al interior de la organización.

Reportar oportunamente los incidentes o eventos de seguridad de la información y cualquier comportamiento anormal que se presente en la organización o en sus activos de información.

- Comité de SGSI

Debe mantener constante capacitación y sensibilización a los funcionarios, contratistas y demás partes interesadas en cuanto al reporte de incidentes de seguridad de la información y vulnerabilidades de los sistemas de información con los que cuenta la organización, haciendo énfasis en:

a) Los riesgos de un control de seguridad ineficaz;

b) Que es la violación de la integridad, confidencialidad o expectativas de disponibilidad de la información.

c) Los errores humanos.

d) Las no conformidades con políticas o directrices.

e) Violaciones de acuerdos de seguridad física.

f) El mal funcionamiento en el software o hardware.

g) Las violaciones de acceso.

5.2- Tipos de incidentes de SI

Las partes interesadas del SGSI deben conocer y saber identificar los incidentes definidos por VIDA:

- Acceso no autorizado a la información.
- Divulgación de información sensible.
- Denegación del servicio.
- Daño de la información.
- Ataques externos o internos.
- Ataques dirigidos y no dirigidos
- Pérdida o robo de la información.
- Modificación no autorizada.
- Información no actualizada.
- Mala gestión del conocimiento.
- Daños sobre Activos de información
- Uso indebido de Activos de información
- Uso Indebido de Software

- Uso Indebido de Usuarios
- Suplantación de la organización
- Interrupción de servicios contratados
- Incidentes negativos de proveedores respecto de SI

El Oficial de SGSI debe atender de manera inmediata el incidente de Seguridad de la Información, de acuerdo a los niveles de criticidad del evento / incidente a fin de darle el tratamiento adecuado.

Nivel de criticidad	Descripción
Alto	Interrumpe seriamente la operación de la organización, el incidente puede tener velocidad significativa/rápida en su propagación y ocasionar daños de activos. Podría llegar a afectar más de un tipo de activo.
Medio	Interrumpe en un periodo corto de tiempo los procesos generales de la organización, el incidente/evento compromete un activo importante.
Bajo	No interrumpe los procesos generales de la organización, el incidente/evento, se detecta y puede controlar fácilmente con recursos existentes en la organización.

El Oficial de SGSI atiende el incidente de Seguridad de la Información, de acuerdo a la siguiente tabla de escalamiento a fin de darle el tratamiento adecuado

Relevancia	Escalamiento
Alto	Se escala a los proveedores pertinentes y si es el caso a las autoridades externas competentes
Medio	Se escala al Comité de SGSI, Área de Infraestructura (mesa de servicios internos) y a las áreas involucradas
Bajo	Solo se diligencia el caso en la herramienta de ticket del área de infraestructura, o se escala al responsable del activo de información involucrado en caso de ser necesario.

El área de Infraestructura para preservar la Integridad, Disponibilidad y Confidencialidad de los activos de información debe generar las alertas tempranas mediante las herramientas tecnológicas disponibles así:

- Grupo de Infraestructura y soporte: Alertas de la infraestructura de T.I. Alertas de las plataformas de información.
- Comité de SI: Alertas de activos de Seguridad, Alertas de fuga de información.

5.3 Tratamiento

Actividades	Descripción	Responsable
Reportar el incidente de seguridad	Los funcionarios, contratistas y demás partes interesadas con acceso a información de la organización detectan que se está presentando un ataque a los activos de la organización, o es conocedor de que alguna persona está violando las políticas de	Los funcionarios, contratistas y demás partes interesadas

Actividades	Descripción	Responsable
	seguridad de la información o conoce de riesgos asociados a la información, debe proceder a reportar esta situación como un evento o incidente de seguridad al Oficial de SI de VIDA: • enviando un correo a OficialSI@VIDA.com.uy • llamando a la Extensión 214 • o informando directamente al Oficial de Seguridad	Mesa de Servicios Internos
Registrar evento o incidente	Mesa de servicios internos toma los datos necesarios y realiza el registro correspondiente en la gestión de incidentes categorizando si se trata de incidente o evento, fecha y hora, pequeña descripción de lo ocurrido, si se puede solucionar de inmediato se documenta la solución aplicada entre otros. Nota: se registran incidentes provenientes de notificación de herramientas que lo ameriten (por ejemplo: reporte de firewall, análisis de infraestructura, etc.)	Mesa de Servicios internos
Evaluar el impacto	Dado el caso que Mesa de Servicios Internos no pueda resolver el evento/incidente se escala al segundo nivel donde el Oficial del SGSI o quien haga sus veces evaluará que tipo de evento/incidente es el que se presenta, a que activos está afectando, cual es alcance del mismo, que pronóstico tiene de expansión, así como los daños potenciales o reales que se generen. Para evaluar la severidad de los eventos/incidentes considerará la relevancia de los activos y el nivel del incidente. Cuando exista la convivencia de más de un activo comprometido y/o más de un incidente o evento, todo el conjunto se valorará de acuerdo a los niveles descritos en la Tabla 1 del presente procedimiento y teniendo en cuenta la relevancia del activo.	Oficial de Seguridad de la información.
Identificar la relevancia del activo	De acuerdo a la verificación de los riesgos asociados a los activos de información que se encuentran en el procedimiento de evaluación de riesgos, se establecerá la afectación del activo de información, incluyendo la cantidad información relevante para la empresa contenida en el mismo.	Oficial de Seguridad de la Información funcionarios, contratistas y demás partes interesadas
Identificar el nivel del incidente	El Oficial de Seguridad de la Información o quien haga sus veces, deberá identificar el nivel de afectación del incidente de acuerdo a los Niveles de Criticidad del Evento/Incidente descritos en la Tabla 1 de la presente guía.	Oficial de Seguridad de la Información
Escalar el incidente	Para buscar una solución al incidente el Oficial de Seguridad de la Información o quien haga sus veces debe tener en cuenta los niveles de escalamientos Tabla 2 de la presente guía.	Oficial de Seguridad de la Información
Establecer la estrategia de respuesta de acción ante incidentes de Seguridad de la Información	Para saber cómo actuar ante un incidente el Oficial de Seguridad de la Información o quien haga sus veces y el área encargada de gestionar el incidente de seguridad, conforme al nivel de evento/incidente establece el tipo de respuesta. Tener en cuenta las autoridades y los grupos de interés descritos en el Manual de Controles	Comité de SI
Iniciar la estrategia de Contención	El Oficial de Seguridad de la Información o quien haga sus veces junto al área encargada de gestionar el incidente de seguridad, deben tener en cuenta los siguientes factores para la contención	

Actividades	Descripción	Responsable
	del incidente o evento • Daño potencial de recursos a causa del incidente. • Necesidad de preservación de la evidencia. • Tiempo y recursos necesarios para poner en práctica la estrategia. • Efectividad de la estrategia. • Duración de las medidas a tomar. • Criticidad de los sistemas afectados. • Características de los posibles atacantes. • Si el incidente es de conocimiento público. • Pérdida económica. • Posibles implicaciones Legales.	Comité de SI
Recolectar evidencia	Para hacer una correcta recolección de evidencia el Oficial de Seguridad de la Información o quien haga sus veces y el área encargada de gestionar el incidente de seguridad, deben tener en cuenta lo siguientes criterios para la recolección de evidencia: • Información basada en la red: Logs de IDSs, logs de monitoreo, información recolectada mediante Sniffers, logs de routers, logs de firewalls, información de servidores de autenticación. • Información Basada en el Equipo: Live data collection: Fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la tarjeta de red. Otra información: Testimonio de funcionario o contratista que reporta el evento o incidente.	Comité de SI
Manejar la evidencia	El Oficial de Seguridad de la Información o quien haga sus veces junto al área encargada de gestionar el incidente de seguridad debe darle un correcto manejo a los datos y evidencias recolectadas, los cuales deben ser almacenados para futuras investigaciones e implementación de controles preventivos o de mejoramiento. La información que debe ser almacenada y custodiada por el Oficial de Seguridad de la Información incluye: • Cantidad de incidentes presentados y tratados. • Daños ocasionados. • Vulnerabilidades explotadas. • Cantidad de activos de información involucradas. • Frecuencias de ataques. • Pérdidas. Además, debe cumplir con un control de seguridad que garantice la confidencialidad, integridad y disponibilidad de las evidencias retenidas. El almacenamiento seguro de las evidencias estará custodiado por	Comité de SI

Actividades	Descripción	Responsable
	el Oficial de seguridad de la información	
Identificar las fuentes de ataque	El área encargada de gestionar el incidente de seguridad, debe tener identificadas las posibles fuentes de ataque posteriormente mencionadas: • Empleados Descontentos. • Baja Concientización. • Crecimiento de Redes. • Falta de Previsión de Contingencias. • Falta de Políticas. • Desastres Naturales. • Inadecuada protección de la Infraestructura. • Confianza creciente en los sistemas. • Virus. • Troyanos. • Explotación de Vulnerabilidades, tanto a nivel de host, como de arquitectura de red (vulnerabilidades de la seguridad perimetral). • Falsificación de identificadores (biométricas, de autenticación o de encabezado de paquetes). • Robo de Información confidencial. • Violación a la privacidad. • Ingeniería social. • Denegación de Servicios. • Hacking.	Comité de SI
Establecer la estrategia de Erradicación	El área encargada de gestionar el incidente de seguridad, debe tener en cuenta para definir/decidir las estrategias de erradicación los siguientes factores: •Tiempo y Recursos necesarios para poner en práctica la estrategia. •Efectividad de la Estrategia. •Pérdida económica. •Posibles implicaciones legales. •Relación costo-beneficio de la estrategia. •Experiencias anteriores. •Identificación de los Procedimientos de cada sistema Operativo comprometido. •Identificación de Usuarios o servicios comprometidos para proceder a desactivarlos.	Comité de SI
Aplicar los procedimientos de Recuperación	El área encargada de gestionar el incidente de seguridad, para definir/decidir las estrategias de recuperación debe tener en cuenta los siguientes factores: • Cargar la copia de respaldo actualizada del sistema de	Comité de SI

Actividades	Descripción	Responsable
	información, configuración o base de datos. • Creación nuevamente de la información digital o física, configuración de sistemas operativos, sistemas de información, cargue manual de la información. • Actualización, instalación de parches de seguridad a los sistemas que se vieron comprometidos. Entre otras definidas en el Plan de Contingencias	
Realizar el análisis Post-Incidentes	El Oficial de Seguridad de la Información o quien haga sus veces debe garantizar el correcto manejo de las lecciones aprendidas, de la siguiente manera: • Periódicamente el Oficial de Seguridad de la Información o quien haga sus veces se reunirá con el área de Mesa de Servicios Internos a fin de analizar los eventos e incidentes presentados durante el periodo. Se busca definir esquemas más efectivos para responder ante situaciones que afecten la seguridad de la información en la organización. Entre las actividades que se realizan está: • Mantener la documentación de los eventos e incidentes de seguridad de la Información. • Integrar los eventos e Incidentes a la Matriz de Riesgos de los Activos. • Realización de Capacitaciones a los funcionarios de la organización en lo relacionado a eventos e incidentes de seguridad de la información. • Analizar los Hechos y tomar decisiones.	Comité de SI

6. Registros

- Gestión de incidentes