1. Objetivo

Definir la clasificación de los incidentes de seguridad de la información como también los logs de auditoría que monitorea y analiza la Cooperativa, de igual manera, los criterios y valores para evaluar los incidentes según su criticidad, impacto y nivel de respuesta.

2. Alcance

Complementar la gestion de incidentes y su respectivo procedimiento con informacion relevante que menciona los diferentes tipos de incidentes, como evaluarlos y con que prioridad antederlos.

3. Términos y Definiciones

3.1 **Prioridad:** Ventaja, Importancia o Preferencia que una persona o cosa tiene sobre otra.

3.2 **Criticidad del Sistema:** Es el impacto e importancia que tiene una máquina, equipo o dispositivo en los procesos de una organización.

3.3 **Impacto Actual:** El daño o afectación que ha generado el incidente en el momento de ser detectado

3.4 **Impacto Futuro:** Daño o afectación que podría generar el incidente si no es contenido ni erradicado.

4. Clasificación de Incidentes

CATEGORIA	DEFINICION	TIPOS	DESCRIPCION-EJEMPLOS
Acceso no autorizado	Ingreso y Operación no autorizada a los sistemas, tanto exitosos como no exitosos.	Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos. Robo de información. Borrado de información. Alternación de la Información. Intentos recurrentes y no recurrentes de acceso no autorizado Abuso y/o Mal uso de los servicios informáticos internos o externos que requieren autenticación.	Además de un abuso local de datos y sistemas, la seguridad de la información puede ser en peligro por una cuenta exitosa o compromiso de la aplicación. Además, son posibles los ataques que interceptan y acceden a información durante la transmisión (escuchas telefónicas, spoofing o secuestro). El error humano / de configuración / software también puede ser la causa.
Código Malicioso	Introducción de códigos maliciosos en la infraestructura tecnológica de la organización.	Virus informáticos. Troyanos. Gusanos informáticos.	Software que se incluye o inserta intencionalmente en un sistema con propósito dañino. Normalmente, se necesita una interacción del usuario para activar el código. / Malware, virus, gusanos, spyware, dialler, rootkit.
Denegación del Servicio	Eventos que ocasionan perdida de un servicio en particular	Ataque de denegación de servicio (DoS / DDoS) Sabotaje Intercepción de información.	Tiempos de respuesta muy altos sin razones aparentes, servició(s) interno(s) inaccesibles sin razones aparentes, Servicio(s) externo(s) inaccesibles sin razones aparentes / Con este tipo de ataque, un sistema es bombardeado con tantos paquetes que las operaciones se retrasan o el sistema falla. Algunos ejemplos DoS son ICMP e inundaciones SYN, ataques de teardrop y bombardeos de mail's. DDoS a menudo se basa en ataques DoS que se originan en botnets, pero también existen otros escenarios como Ataques de amplificación DNS. Sin embargo, la disponibilidad también puede verse afectada por acciones locales (destrucción, interrupción del suministro de energía, etc.), fallas espontáneas o error humano, sin mala intención o negligencia.
Recopilación de información	Eventos que buscan obtener información de la	Scanning	Ataques que envían solicitudes a un sistema para descubrir puntos débiles. Se incluye también algún tipo de proceso de prueba para reunir información sobre hosts, servicios y cuentas. Ejemplos: fingerd, consultas DNS,

	infraestructura tecnológica de la organización		ICMP, SMTP (EXPN, RCPT, …), escaneo de puertos
		Vulnerabilidades	Un intento de comprometer un sistema o interrumpir cualquier servicio explotando vulnerabilidades conocidas que ya cuentan con su clasificación estandarizada CVE (por ejemplo, el búfer desbordamiento, puerta trasera, secuencias de comandos cruzadas, etc).
		Sniffing	Observar y registrar el tráfico de la red (escuchas telefónicas o redes de datos).
		ingeniería Social	Phishing
Mal uso de los Recursos tecnológicos	Eventos que atentan contra los recursos tecnológicos por el mal uso	Mal uso y/o Abuso de servicios informáticos internos o externos	Manejo indebido o abusivo sobre los recursos informáticos de la organización.
		Violación de las normas de acceso a internet	Pornografía infantil, glorificación de la violencia, otros
		Mal uso y/o Abuso del correo electrónico de la organización	«Correo masivo no solicitado», lo que significa que el destinatario no ha otorgado permiso verificable para que el mensaje sea enviado y además el mensaje es enviado como parte de un grupo masivo de mensajes, todos teniendo un contenido similar
		Violación de las Políticas, Normas y Procedimientos de Seguridad Informática establecidas para proteger la información.	Políticas que rigen y se encuentren vigentes dentro de la organización.
Otros		Un incidente no puede clasificarse en alguna de las categorías anteriores.	Este tipo de incidentes debe monitorearse con el fin de identificar la necesidad de crear nuevas categorías.

5. Evaluación del Incidente

5.1 Nivel de Criticidad

Los recursos, sistemas afectados o el origen propio del incidente se deben medir según el impacto e importancia que tengan estos para la Cooperativa. Identificar el nivel de criticidad a partir de la siguiente tabla.

Nivel de Criticidad	Valor	Definición
Inferior	**0,10**	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	**0,25**	Sistemas que apoyan a una sola dependencia o proceso de una entidad.
Medio	**0,50**	Sistemas que apoyan más de una dependencias o procesos
Alto	**0,75**	Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones criticas
Superior	**1,00**	Sistemas Críticos

5.2 Impacto

Luego de medir la **criticidad**, se debe identificar el valor que tendrá el **Impacto actual** y el **Impacto futuro**, según lo descrito en la siguiente tabla.

Nivel de Impacto	Valor	Definición
Inferior	**0,10**	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo
Bajo	**0,25**	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo
Medio	**0,50**	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo
Alto	**0,75**	Impacto moderado en uno o más de los componentes de más de un sistema de información
Superior	**1,00**	Impacto alto en uno o más de los componentes de más de un sistema de información

5.3 Nivel de Prioridad

Por último, una vez definidas las anteriores variables de Criticidad del sistema, Impacto actual y futuro, se calculará la prioridad del incidente mediante la siguiente formula:

Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema*5)

Los resultados obtenidos se deben comparar con la siguiente tabla para determinar la prioridad de atención:

Nivel de Prioridad	Valor
Inferior	**00,00 – 02,49**
Bajo	**02,50 – 03,74**
Medio	**03,75 – 04,99**
Alto	**05,00 – 07,49**
Superior	**07,50 – 10,00**

5.4 Nivel de Respuesta:

Para el caso de la atención de incidentes de seguridad se ha establecido tiempos máximos de atención de estos, con el fin de atender adecuadamente los incidentes de acuerdo con su criticidad e impacto. Los tiempos expresados en la siguiente tabla son un acercamiento al tiempo máximo en que el incidente debe ser atendido, y no al tiempo en el cual el incidente debe ser solucionado. Esto se debe a que la solución de los incidentes puede variar dependiendo del caso.

Según el nivel de prioridad de la anterior tabla, se puede identificar el tiempo máximo en que deberá ser atendido el incidente de seguridad.

Nivel de Prioridad	Valor
Inferior	**3 horas**
Bajo	**1 hora**
Medio	**30 min**
Alto	**15 min**
Superior	**5 min**

CONTROL DE CAMBIOS		
La trazabilidad de los cambios generados en el documento podrá ser consultada en el Listado Maestro de Documentos.		
Versión	**Descripción Del Cambio**	**Fecha de Aprobación**
1	Elaboración inicial del documento	25/04/2023

Elaborado Por:	Revisado Por:	Aprobado Por:
RICARDO MARIA SUAREZ ORTIZ **Cargo:** Subgerente de sistemas	**SERGIO ALEJANDRO CUELLAR CARDONA** **Cargo:** Apoyo Transf. Digital y SIG	**NÉSTOR BONILLA RAMÍREZ** **Cargo:** Gerente General