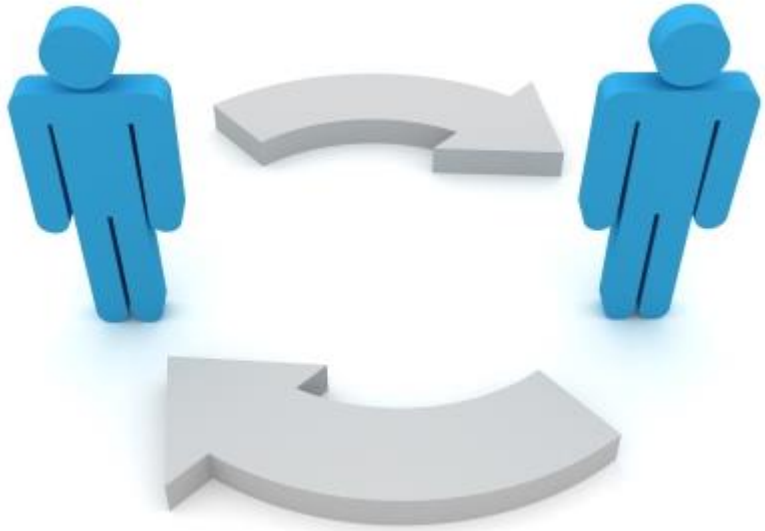
# 7. Controles de Ciberseguridad

## 2. Marco de Compartición de Información

### 2.1 Introducción

Los incidentes de ciberseguridad a menudo **cruzan las fronteras** geográficas nacionales y de organización, y la **velocidad** a la que fluye la información y los **cambios** que se desarrollan en el incidente dan tiempo limitado para actuar a los individuos y organizaciones que deben responder.



Debe establecerse un **sistema para el intercambio de información** y coordinación para ayudar a preparar y responder a los eventos e incidentes de ciberseguridad. Este es un paso importante que las organizaciones deben tomar como parte de sus controles de seguridad. Este sistema de intercambio de información y la coordinación debe ser segura, eficaz, fiable y eficiente.

El **sistema debe ser seguro** para garantizar que la información que se comparte, incluyendo detalles sobre la coordinación de las actividades, están protegidos contra accesos no autorizados, en particular para el autor de los hechos en cuestión.

También es necesaria la seguridad de la información relativa a los acontecimientos de ciberseguridad para evitar interpretaciones erróneas o causar pánico o alarmas indebidas al público.

Al mismo tiempo, **la integridad y la autenticidad de la información** son fundamentales para asegurar su exactitud y fiabilidad, independientemente de si dicha información es compartida dentro de un grupo cerrado, o revelado públicamente.

El **sistema debe ser eficaz y eficiente**, de modo que sirva a su propósito con un mínimo de recursos y en el tiempo requerido y el espacio.

En este módulo establecemos un marco básico para la implementación de un sistema de intercambio y coordinación de información.

El marco incluye cuatro áreas para su consideración:

- Políticas
- Métodos y procesos
- Personas
- Elementos técnicos.

## 2.2 Políticas

### 2.2.1 Organizaciones Proveedoras y Receptoras de Información

A los efectos de este marco, se introducen dos tipos de organizaciones de intercambio de información:

- IPO
- IRO

Como IPO, deben determinarse las **políticas básicas** con respecto a la clasificación y categorización de la información, la gravedad de los acontecimientos e incidentes, y la forma de compartición, antes de la ocurrencia de cualquier incidente de seguridad, o antes de que cualquier intercambio tenga lugar (en el caso de que una IPO se convierta en una IRO para compartir la información recibida con otras entidades autorizadas en la cadena de información).

En el extremo receptor, una IRO debe ponerse de acuerdo para hacer **cumplir la protección de seguridad y los procedimientos pertinentes** al recibir información de una IPO, de conformidad con el acuerdo alcanzado previamente, y en base a la clasificación y categorización de la información involucrada.

### 2.2.2 Clasificación y Categorización de Información

Las IPO deben determinar las diferentes **categorías de información** que se recopilará, cotejará, custodiará y distribuirá. Ejemplos de categorías de información pueden incluir eventos de seguridad, amenazas de seguridad, vulnerabilidades de seguridad, perfiles de atacantes sospechosos/confirmados, grupos organizados, víctimas, y categorías de perfil de sistema ICT.


Cada categoría debe subdividirse en dos o más clasificaciones basadas en el contenido de la información en cuestión.

La clasificación mínima puede ser sensible y sin restricciones.

Si la información contiene datos personales, debe aplicarse también **clasificaciones de privacidad**.

### 2.2.3 Minimización de Información

Para cada categoría y clasificación, la IPO debe tener cuidado de **reducir al mínimo la información que se distribuye**. La reducción al mínimo es necesaria para evitar la sobrecarga de información en el extremo de recepción y para asegurar el uso eficiente del sistema de reparto sin comprometer la eficacia. Otro objetivo de la minimización es omitir información importante para preservar la privacidad de las personas en IPO e IRO. En este respecto, **IPO e IRO deben determinar el nivel deseado de detalle**, siempre que sea posible, para cada categoría y clasificación.

### 2.2.4 Audiencia Limitada

En línea con el principio de minimización, debe establecerse una política para limitar la audiencia, que puede ser una persona específica de contacto, un grupo u organización, a las que distribuir información que contiene datos privados o confidenciales.


Para información menos sensible, esta política debe tenerse en cuanta para evitar la sobrecarga de información, a menos que los beneficios de la máxima distribución (como el uso compartido de las alertas de seguridad críticas) sean mayor que el impacto de la sobrecarga de información para la IRO.

### 2.2.5 Protocolo de Coordinación

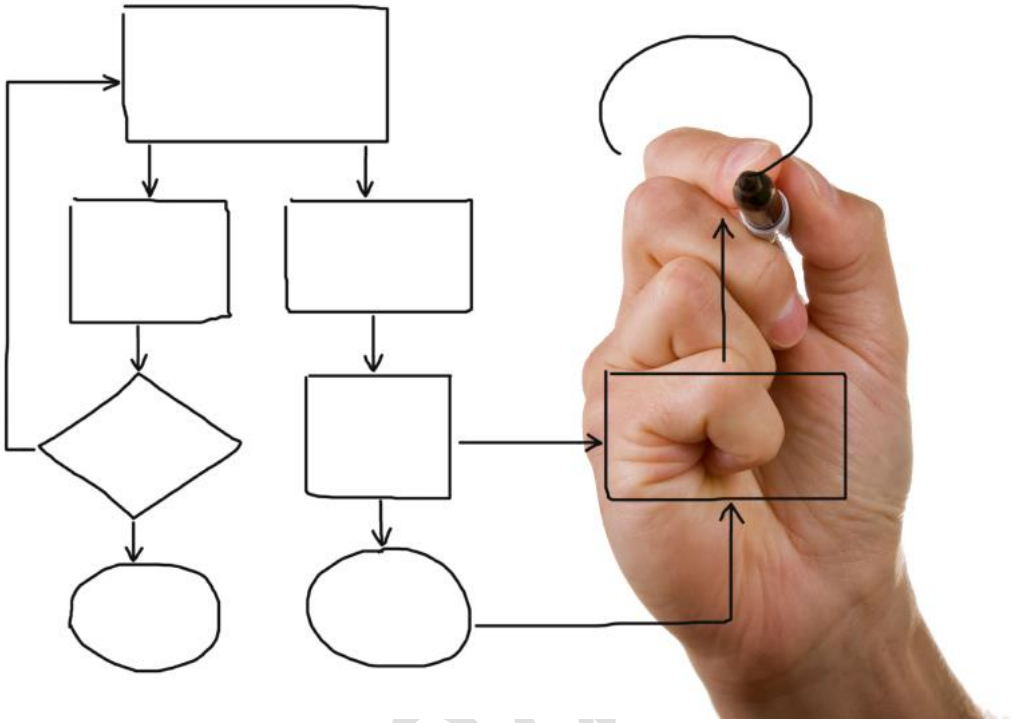
Debe establecerse una **política de alto nivel para coordinar la solicitud y distribución** (tanto si se inicia por una IPO como una IRO).

Esta política formaliza el protocolo implicado, que proporciona un medio para la IPO y la IRO para responder con eficacia y eficiencia.

Pueden construirse procedimientos de autenticación mutua y verificación sobre el protocolo para asegurar la autenticidad del origen y la prueba de la entrega cuando se desee, en particular, para la información sensible, personal y/o confidencial.

### 2.3 Métodos y Procesos

Para llevar a cabo las políticas de intercambio de información, y garantizar la coherencia, la eficacia, la eficiencia y la fiabilidad de la ejecución, deben desarrollarse métodos y procesos.



**Tales métodos y procesos deben basarse en estándares disponibles**.

Las cláusulas siguientes proporcionan orientación sobre los métodos y procesos que son comúnmente utilizados por las organizaciones para lograr los objetivos y políticas pertinentes de intercambio de información y la coordinación en el contexto de la ciberseguridad.

#### 2.3.1 Clasificación y Categorización

La información a ser compartida vendrá tanto de **fuentes abiertas como cerradas**.

La información de fuente abierta es la que se encuentra en Internet o en otras fuentes públicas, tales como los periódicos. La información de fuente abierta tendrá generalmente una clasificación más baja, ya que los autores de la información pueden ser múltiples o desconocidos, la antigüedad de la información puede ser indeterminada y la precisión puede ser cuestionable.

La información de fuente cerrada no está disponible al público, a menudo es atribuible a una fuente y de antigüedad conocida.

Ejemplos de información de código cerrado son la investigación privada y análisis, o la inteligencia empírica recolectada.

### 2.3.2 Acuerdo de No Divulgación

Se puede utilizar un **NDA (Non-disclosure agreement)** por lo menos para dos propósitos en el contexto del intercambio de información y la coordinación para mejorar la ciberseguridad.


Un uso típico de un NDA es **garantizar el manejo adecuado y la protección** de la información sensible, personal y/o confidencial compartida entre IPO e IRO, y establecer las condiciones de compartición y de su posterior distribución y el uso de dicha información.

En el contexto de responder a los eventos de ciberseguridad, el establecimiento de un acuerdo de confidencialidad permite que se **lleve a cabo de manera eficiente el intercambio rápido** y la distribución entre las entidades autorizadas, incluso si la clasificación de la información no ha sido claramente definida.

### 2.3.3 Código de Práctica

Un método comúnmente usado para asegurar una distribución adecuada y el manejo de la información sensible es el **establecimiento de un código de prácticas**, que comprenda procedimientos detallados, responsabilidades y compromisos de las organizaciones interesadas (es decir, IPO e IRO) para las respuestas y acciones a ser tomadas por las respectivas entidades para cada categoría y clasificación de la información.

Ver el estándar **ISO/IEC 29147**, Information technology – Security techniques – Vulnerability disclosure.

### 2.3.4 Pruebas y Simulaciones

Para garantizar la eficacia y fiabilidad y para alcanzar el nivel deseado de eficiencia, los métodos y los procesos deben ser desarrollados de forma que **se puedan realizar pruebas regulares y se puedan practicar los escenarios descritos**.

Debe usarse una metodología estándar como referencia para las pruebas de seguridad, con el fin de adaptarse a los objetivos y necesidades de la organización.

Las pruebas de seguridad se pueden realizar en activos de alto riesgo. A esto puede ayudar el uso de la nomenclatura y clasificación de los datos propia de la organización.

Las evaluaciones de seguridad deben realizarse de forma regular en:

- Aplicaciones
- Sistemas operativos
- Sistemas de Gestión de Base de Datos

### 2.3.5 Calendario y Programación del Intercambio

La obligación de compartir información, ya sea de forma proactiva o durante la respuesta a un incidente puede variar de una entidad a otra. Algunas organizaciones tienen una necesidad de información en tiempo real: se desea obtener la información en el momento de alerta o alarma para su posterior análisis. Otras entidades no poseen los recursos para gestionar en tiempo real la información compartida. **El calendario y la programación del intercambio de información deben estar claramente definidos**, con objetivos específicos de nivel de servicio definidos por relaciones voluntarias y acuerdos de nivel de servicio para relaciones comerciales.

## 2.4 Personas y Organizaciones

Las personas y las organizaciones son los principales factores determinantes del éxito de la ciberseguridad. Para la eficacia y la eficiencia, deben considerarse las necesidades de las personas y las organizaciones.

### 2.4.1 Contactos

Debe **compilarse una lista de contactos por parte de la IPO y la IRO** y debe intercambiarse de manera que cada entidad pueda identificar a la persona que solicitó o envió información.


También pueden desarrollarse y distribuirse listas de contactos más granulares de conformidad con una audiencia limitada y las políticas de clasificación y categorización de la información.

La lista de contactos **no debe contener información personal sensible**, de conformidad con la política de minimización de la información. Por razones de privacidad, podría considerarse el uso de alias en lugar del nombre completo.

La información mínima para la lista de contactos debe incluir el nombre (o alias), los números de teléfono móvil de contacto (si es posible), y la dirección de correo electrónico. También puede establecerse un **contacto alternativo** para cada persona clave en la lista de contactos.

Además de una lista de contactos para el intercambio de información y coordinación, también **puede recopilarse una lista de contactos diferente para el escalado del incidente**. Dicha lista incluye generalmente contactos externos que no están en la red de intercambio.

Como mínimo, la lista de contactos debe ser protegida contra modificaciones no autorizadas para prevenir la corrupción y mantener la integridad. Deben aplicarse los controles técnicos que veremos más adelante.

### 2.4.2 Alianzas

Para facilitar el intercambio de información y establecer prácticas comunes y coherentes regidas por un código de práctica acordado, y/o NDA, las organizaciones y los grupos de individuos

**pueden formar alianzas** basadas en sus áreas de interés, que pueden ser la industria, la tecnología, u otras áreas de interés.

### 2.4.3 Concienciación y Formación

Las personas en las organizaciones deben ser **conscientes de los nuevos riesgos emergentes en ciberseguridad** y deben ser entrenados para que desarrollen las habilidades y experiencia requeridas para responder eficaz y eficientemente cuando se encuentran con un riesgo específico.

Para lograr estos objetivos,

- Deben organizarse **sesiones informativas periódicas** sobre el estado de ciberseguridad referente a la organización y la industria.
- Deben diseñarse y organizarse **sesiones de entrenamiento con simulaciones de escenarios de ataque** y talleres sobre áreas de acción específicas.
- Debe llevarse a cabo la **comprobación periódica, con escenarios pertinentes** para asegurar la comprensión global y la capacidad de ejecutar procedimientos y herramientas específicas.

Esta toma de conciencia, la formación y las pruebas pueden ser realizadas por expertos internos, consultores externos, u otros expertos de los miembros de las alianzas vinculadas que participan en el intercambio de información y coordinación.

El uso de escenarios como parte de los procesos de formación y las pruebas que se recomiendan permiten a las personas a tener experiencia cercana a la vida real de situaciones relevantes y aprender y practicar las respuestas requeridas. Además, **los incidentes pasados pueden ser utilizados como parte de los escenarios** para maximizar el intercambio de lecciones aprendidas y la comprensión adquirida en esas situaciones.

## 2.5 Elementos Técnicos

Los controles técnicos y la normalización se pueden utilizar para **mejorar la eficiencia, reducir los errores humanos y mejorar la seguridad en el intercambio de información** y los procesos de coordinación.

Pueden diseñarse, desarrollarse e implementarse sistemas y soluciones técnicas. Esta Norma Internacional proporciona algunos de los enfoques utilizados y las técnicas que han sido adoptadas por algunas organizaciones, y pueden ser adaptadas además para mejorar el intercambio de información y las necesidades de los procesos de coordinación para hacer frente al riesgo de ciberseguridad en un entorno cambiante.

### 2.5.1 Estandarización de Datos

Como parte de la red de distribución, pueden **desarrollarse y desplegarse sistemas automatizados** entre las organizaciones coordinadas **para recopilar datos sobre la evolución de los acontecimientos de ciberseguridad**, para el análisis en tiempo real y fuera de línea y la evaluación, con el fin de determinar el estado de seguridad más reciente en el ciberespacio dentro de los límites de la organizaciones involucradas.


Estos datos pueden incluir datos de **tráfico de red**, **actualizaciones de seguridad** para los sistemas de software y dispositivos de hardware, **datos de vulnerabilidades** de seguridad y **malware**, **spam**, programas espía, incluyendo sus payloads e información interceptada.

Los sistemas automatizados también contienen datos relativos a las organizaciones y personas. En vista de la sensibilidad y el volumen de los contenidos de los datos involucrados en estos sistemas, las organizaciones (en particular, las alianzas de organizaciones) deben evaluar los esquemas de datos y contenidos adecuados para determinar los controles técnicos para mejorar la eficiencia, la eficacia y la seguridad.

Estos pueden incluir, pero no se limitan a:

a) **Estandarización del esquema de datos para cada categoría y clasificación** de los datos recogidos de forma que cumpla la minimización de la información y la política de privacidad, y asegure la disponibilidad a todas las entidades participantes

b) **La estandarización del formato de datos para facilitar el intercambio** y mejorar el almacenamiento, transporte, manipulación y la interoperabilidad entre los sistemas. Por ejemplo, véase UIT-T X.1205

c) La **estandarización de la funcionalidad básica** de procesamiento de datos y los algoritmos utilizados, por ejemplo, la función **hash** y los procedimientos para la **anonimización** de la dirección IP y otros requisitos de preprocesamiento.

### 2.5.2 Visualización de Datos

Debe considerarse el uso de técnicas de visualización de datos para presentar información de eventos, lo que ayuda a mejorar la visibilidad de los cambios sin la necesidad de que los operadores tengan que leer los detalles de cada evento a medida que ocurren.

### 2.5.3 Intercambio de Claves y Backups

Para facilitar el intercambio de información confidencial, debería considerarse **un sistema criptográfico**, incluyendo un **sistema de intercambio de claves**.

El sistema debe incluir copias de seguridad adecuadas para el software y hardware, así como las claves utilizadas en la preparación para los propósitos de compartir y las necesidades de recuperación de emergencia.

### 2.5.4 Compartición segura de archivos, mensajería instantánea, portal web y foros de discusión

Para facilitar la interacción en línea y el intercambio de información rápido y seguro, que puede incluir la distribución de contenidos digitales como archivos de texto y multimedia, y los debates en línea y fuera de línea, las organizaciones (IPO y IRO) deberían considerar la adopción de **herramientas adecuadas para compartir archivos, mensajería instantánea y herramientas en**

**línea para foros de discusión** que podrían satisfacer la seguridad, eficacia, eficiencia, fiabilidad y necesidades.

Debería implementarse un **portal web con feeds sobre eventos de ciberseguridad** como una forma de comunicación para la comunidad.

Cuando dicho portal web se utiliza, debe haber una clara propiedad administrativa y la responsabilidad de velar por su seguridad y disponibilidad, y deben facilitarse áreas privadas para una audiencia limitada cuando sea necesario.

### 2.5.5 Prueba de Sistemas

Ya que cada sistema técnico y los métodos y procesos relacionados **deben ser probados rigurosamente** para asegurar su fiabilidad y la integridad, deberían considerarse uno o más sistemas técnicos dedicados para mejorar la eficiencia y eficacia de la prueba, en particular, las pruebas de escenarios.

Tal sistema puede estar en la forma de un **sistema de simulación para simular los entornos operativos** percibidos por cada organización, y la evolución de la situación de ciberseguridad, que proporcione la capacidad para la introducción de una serie de eventos de seguridad para facilitar la prueba a realizar.

### 2.6 Guía de Implementación

La puesta en práctica de este marco requiere que las organizaciones e individuos colaboren para conseguir juntos determinar políticas específicas, controles y los pasos a seguir a fin de lograr sus objetivos de intercambio de información segura, eficaz, confiable y eficiente y la coordinación en la respuesta a los nuevos incidentes de seguridad cibernética.

Se recomiendan los siguientes pasos de alto nivel como una guía para la aplicación:

a) Identificar y reunir las organizaciones y los individuos que van a formar parte del intercambio de información necesaria y de la red de coordinación de la comunidad, ya sea formal o informal;

b) Determinar el rol de cada organización/individuo involucrado, ya sea como IPO, IRO, o ambos

c) Establecer el tipo de información y coordinación que se requiere y que sería beneficioso para la comunidad;

d) Realizar la categorización y clasificación para determinar la información sensible y/o información de privacidad que está involucrada

e) Establecer las políticas y principios que rigen la comunidad y la información implicada

f) Determinar los métodos y procesos requeridos para cada categoría y clasificación de la información implicada

g) Determinar las necesidades de rendimiento y los criterios y establecer el Código de Práctica y firmar el NDA cuando sea necesario

h) Identificar los estándares requeridos y adecuados y los sistemas técnicos para apoyar la implementación y el funcionamiento de la comunidad

i) Prepararse para el funcionamiento: recopilar la lista de contactos, realizar talleres de sensibilización y formación para preparar a los interesados

j) Realizar inspecciones periódicas, incluyendo tutoriales y escenarios de simulación, según sea necesario

k) Realizar revisiones periódicas, post-test y post-incidente para mejorar los sistemas de intercambio y coordinación, incluidas las personas, los procesos y la tecnología de que se trate; ampliar o reducir el tamaño de la comunidad cuando sea necesario.