Cultura de ciberseguridad en la aviación civil

Publicado bajo la responsabilidad del Secretario General

Enero de 2022

Organización de Aviación Civil Internacional

S21-2977

1. Introducción

Esta orientación es cónsona con la Estrategia de Ciberseguridad de la Aviación de la OACI[1] y el Plan de Acción de Ciberseguridad[2], en cuya acción CyAP7.1 se recomienda definir y promover una cultura de seguridad en la aviación civil.

2. Alcance

Este texto de orientación tiene por finalidad ayudar a los Estados miembros y otras partes interesadas a diseñar y poner en práctica una cultura de ciberseguridad sólida en sus respectivas organizaciones. El objetivo último es fortalecer la seguridad y la resiliencia de la aviación civil frente a las ciberamenazas y los ciberriesgos.

3. Definición, objetivos generales y beneficios de la cultura de ciberseguridad

3.1 A los fines de la presente orientación, se entiende por cultura de seguridad el conjunto de supuestos, actitudes, creencias, comportamientos, normas, percepciones y valores que son inherentes a la operación diaria de una organización y que se reflejan en las acciones y comportamientos de todas las entidades y el personal en su interacción con activos digitales.

3.2 Una cultura de ciberseguridad positiva procura hacer que las consideraciones de ciberseguridad formen parte de los hábitos, las conductas y los procesos de la organización, incorporándola en las operaciones diarias para que se refleje en las acciones y comportamientos de todo el personal.

3.3 El establecimiento de una cultura de ciberseguridad fuerte y eficaz como parte integral de la cultura de una organización ayuda a esta a mejorar su desempeño general mediante la detección temprana de posibles ciberriesgos.

3.4 La cultura de ciberseguridad en la aviación civil aprovecha las experiencias, los esfuerzos y los éxitos del sector en la implantación de culturas sólidas en el ámbito de la seguridad operacional y la seguridad de la aviación, y comparte muchos elementos básicos con ellas. Esta naturaleza transversal de la cultura de ciberseguridad no solo contribuye a mejorar la postura de ciberseguridad, sino que además genera efectos secundarios positivos en los tres ámbitos al facilitar la promoción y el reforzamiento de culturas positivas de seguridad operacional, seguridad de la aviación y ciberseguridad.

3.5 En resumen, la cultura de ciberseguridad permite a cada persona de la organización, independientemente de su función, desempeñarse mejor en el entorno digital. Como ejemplos de los beneficios de diseñar e implantar una cultura de ciberseguridad sólida cabría mencionar los siguientes:

a) mayor madurez de la organización en materia de ciberseguridad;
b) manejo apropiado de la información por parte de todo el personal;
c) mejor posición de la ciberseguridad para incrementar la eficacia y eficiencia de la organización para mitigar los ciberriesgos;
d) mayor conciencia de todo el personal ante los ciberriesgos y el papel que cada funcionaria/funcionario desempeña para detectar y atenuar dichos riesgos; y
e) disposición a ejercer la vigilancia personal en la aplicación de procesos y procedimientos de ciberseguridad, así como a notificar toda ciberactividad sospechosa, lo que permitiría actuar de manera proactiva y mejorar la detección de ciberriesgos.

---

[1] https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx.
[2] Comunicación de la OACI núm. 2020/114.

3.6 En las secciones que siguen de la presente orientación se presentan los elementos básicos de una cultura institucional eficaz de ciberseguridad en la aviación. Ahora bien, aunque estos elementos básicos están bien definidos, la cultura de ciberseguridad debería diseñarse de forma específica al interior de cada organización. Esa cultura debería tener en cuenta diferentes aspectos, como el nivel de madurez de la ciberseguridad institucional, las culturas y los valores existentes y el contexto general de amenazas a la ciberseguridad.

3.7 Los elementos básicos de una cultura de ciberseguridad sólida y eficaz en la aviación civil son:

a) liderazgo;
b) vínculos transversales;
c) comunicación;
d) concienciación, instrucción y educación;
e) sistemas de notificación;
f) examen y mejoramiento continuos; y
g) ambiente laboral positivo.

4. **Liderazgo**

4.1 La eficacia de la cultura de ciberseguridad depende del compromiso de cada persona integrante de la organización, comenzado con la administración superior. La administración superior debería aportar su pleno compromiso con la cultura de ciberseguridad, en todo momento y en todas las actividades, estrategias, políticas y objetivos institucionales.

4.2 La administración superior debería cumplir con las políticas de ciberseguridad, predicar con el ejemplo y servir de modelo para los directores y el personal de la organización. También debería abogar por la ciberseguridad como valor institucional y personal y, al mismo tiempo, trabajar por que sus comportamientos sean cónsonos con dicho valor.

4.3 En tal sentido, la administración superior debería:

a) esforzarse por ampliar sus conocimientos sobre la ciberseguridad en la aviación civil;
b) ceñirse a las reglas, procesos y procedimientos de ciberseguridad en todo momento y predicar con el ejemplo;
c) incluir claramente la ciberseguridad como prioridad institucional;
d) consagrar la ciberseguridad de la aviación en las políticas escritas de la organización de forma que se convierta en parte integral del plan de gestión de la institución;
e) brindar un respaldo visible a la implantación de una cultura de ciberseguridad;
f) asegurar y facilitar la instrucción y capacitación de todo el personal en materia de ciberseguridad;
g) cuidar del procesamiento oportuno de las notificaciones de ciberseguridad y de la pronta ejecución de toda medida correctiva y preventiva que se requiera;
h) intervenir debidamente siempre que la ciberseguridad se vea comprometida; y
i) vigilar tanto el desarrollo de la postura y la cultura de ciberseguridad de la organización como las medidas y recursos asignados para contribuir al mejoramiento continuo de la adopción de dicha cultura en toda la organización.

4.4 Siguiendo el ejemplo de la administración superior, los otros niveles de administración de la organización también deberían procurar adoptar las medidas indicadas en el párrafo 4.3, en consonancia con sus responsabilidades y ámbito de gestión, a fin de propagar el compromiso con la cultura de ciberseguridad en toda la organización.

5. **Vínculos transversales**

5.1 Habida cuenta del gran número de ciberriesgos y vulnerabilidades en toda organización, deberían establecerse formalmente vínculos transversales.

5.2 Podría instituirse un equipo especial multidisciplinario que rinda cuentas directamente a la administración superior como medida para facilitar la coordinación de la cultura de ciberseguridad en toda la organización.

5.3 Los objetivos del equipo especial serían los siguientes:

a) evaluar periódicamente la madurez de la cultura de ciberseguridad en la organización;
b) definir los riesgos y oportunidades de la implantación de una cultura de ciberseguridad;
c) conectar las perspectivas de las diferentes partes interesadas internas en cuanto a la cultura de ciberseguridad; y
d) contribuir a la formulación y ejecución de actividades transversales para fomentar una cultura de ciberseguridad en la organización.

6. **Comunicación**

6.1 La comunicación cumple una función esencial, tanto interna como externamente, para asegurar la implantación de una cultura de ciberseguridad exitosa. Es el principal medio para alcanzar el nivel de concienciación esperado.

6.2 Para lograr una comunicación eficaz, deberían considerarse ciertas aptitudes como parte de una cultura de ciberseguridad sólida:

a) *escucha activa*: proceso por el cual se observan las señales verbales y no verbales a fin de reconocer los valores y las necesidades de la otra persona y contribuir al mejoramiento de la comunicación en el equipo;
b) *adaptación del estilo de comunicación a las distintas audiencias y situaciones*: entender cómo se comunican otras personas y ajustar el mensaje para que les llegue mejor; y
c) *claridad de la comunicación*: determinar qué comunicar y cómo hacerlo.

6.3 La administración superior debería asegurarse de que las políticas y directrices internas relativas a la ciberseguridad, así como las razones de su introducción, sean debidamente comunicadas a todo el personal. Un programa sólido de comunicación interna contribuye a la comprensión y aceptación de las medidas de ciberseguridad por parte de todo el personal y ayuda a promover la cultura de ciberseguridad en la organización.

6.4 Además, los programas de comunicación interna serían de gran ayuda para:

a) asegurarse de que todo el personal tenga plena conciencia de sus deberes y derechos y conozca cabalmente los mecanismos de notificación que existen en su organización; y
b) promover el código de conducta digital institucional, el cual incluye los procesos, las medidas y los controles que el personal debería cumplir en todo momento.

7. **Concienciación, instrucción y educación**

7.1 La concienciación, instrucción y educación son áreas clave del proceso de aprendizaje que deberían fortalecerse para alcanzar una cultura de ciberseguridad sólida. La concienciación proporciona a las personas los conocimientos, la instrucción enseña destrezas y la educación brinda conocimientos y destrezas dentro de un marco teórico, por lo que en ella se integran la concienciación y la instrucción.

7.2 Todo el personal de aviación civil que interactúa con los activos digitales de la organización, independientemente de sus responsabilidades o funciones, debería seguir un programa de concienciación, instrucción y educación en materia de ciberseguridad para asegurarse de que cuenta con los conocimientos y las destrezas que se requieren en cuanto a los riesgos, las medidas y los objetivos de la ciberseguridad en la aviación. Estos programas deberían adaptarse a la audiencia, según las necesidades y en la medida de lo posible.

7.3 Deberían realizarse programas de concienciación sobre la ciberseguridad para todo el personal al momento de su contratación, e igualmente ofrecer instrucción periódica. La periodicidad del programa de concienciación debería definirse con base en el nivel de madurez de la cultura de ciberseguridad en la organización, y puede revisarse de acuerdo con el desarrollo de dicho nivel de madurez.

7.4 Se recomienda impartir estos programas de concienciación sobre ciberseguridad al menos una vez de forma presencial (en un contexto de aula física o virtual). La ciberseguridad no es un tema conocido por todo el personal, por lo que a veces resulta difícil de asimilar sin la orientación de un/a profesional. La interacción con un/a especialista en un aula de clases facilita la comprensión de los temas de ciberseguridad, pues permite al instructor o instructora explicar conceptos, procesos, procedimientos y controles de una manera simplificada para que el personal que no tiene mayores conocimientos técnicos pueda comprenderlos; también es una oportunidad para explicar los beneficios que aporta el mejoramiento de la postura de la organización en materia de ciberseguridad y sus efectos positivos sobre la productividad general de sus funcionarias y funcionarios.

7.5 Tras una primera sesión presencial de concienciación/instrucción, las organizaciones pueden considerar el uso de métodos de aprendizaje electrónico (aprendizaje asistido por computadora) para la instrucción periódica. Esta decisión debería tener en cuenta el desarrollo de la cultura de ciberseguridad en la organización, así como los cambios en los procesos, controles y procedimientos de ciberseguridad que se han incluido en la organización en respuesta a la evolución del contexto de ciberriesgos.

7.6 Los programas de concienciación sobre ciberseguridad deben ser impartidos por profesionales que cuenten con el conocimiento técnico necesario. Sin embargo, uno de los problemas que se presentan con los programas de concienciación en temas técnicos es la falta de aptitudes interpersonales de quienes dictan los programas, ya que unas aptitudes para comunicar y convencer adecuadas facilitan en gran medida la interacción con el personal y contribuyen enormemente a lograr su participación y apoyo a la cultura de ciberseguridad. De allí que las organizaciones deberían velar por que las personas a cargo de los programas de concienciación cuenten tanto con el conocimiento técnico como con las aptitudes interpersonales necesarias para motivar cambios de comportamiento en el personal que favorezcan la adopción de la cultura de ciberseguridad.

7.7 Un programa típico de concienciación sobre ciberseguridad debería incluir los temas siguientes:

a) finalidad del programa de concienciación;
b) mecanismos de comunicación existentes en la organización;
c) panorama general de los ciberriesgos para la aviación civil y posibles consecuencias (con ejemplos);
d) controles, procesos y procedimientos de la organización relacionados con la ciberseguridad;
e) función del elemento humano en la protección de la organización contra los ciberriesgos;

f) importancia de que el personal se recuerde mutuamente los principios de ciberseguridad de la organización al observar acciones por parte de sus colegas que no cumplen con la normativa sobre ciberseguridad;
g) panorama de los distintos métodos de explotación de vulnerabilidades en contra de las personas y sus consecuencias (con ejemplos);
h) cómo detectar ciberactividades sospechosas;
i) impacto del exceso de confianza en la organización (con ejemplos);
j) principios de ciberhigiene;
k) manejo apropiado de datos e información sensibles; y
l) mecanismos de notificación, cómo utilizarlos y mecanismos de seguimiento.

7.8 También deberían realizarse campañas periódicas de concienciación sobre la ciberseguridad a manera de recordatorio para reforzar los conocimientos y las aptitudes del personal. A tal efecto, se cuenta con varias herramientas, entre ellas:

a) *herramientas impresas*: como carteles, folletos, volantes, etc. Este tipo de medios puede distribuirse y digerirse con facilidad. Sin embargo, son herramientas pasivas y deben ser actualizadas con frecuencia (con una nueva impresión para cada actualización); y
b) *herramientas en línea*: como correos electrónicos, boletines, mensajes como protectores de pantalla, intranet, videos cortos, páginas de preguntas frecuentes, aprendizaje electrónico (aprendizaje asistido por computadora), etc. La ventaja principal de estas herramientas respecto de las herramientas impresas es que pueden llegar a toda la organización; son relativamente fáciles de actualizar en cuanto a los recursos que se requieren para ello y tienen un bajo costo de producción.

8. **Sistemas de notificación**

8.1 Una pieza fundamental de la cultura de ciberseguridad es la elaboración y aplicación de un sistema interno de notificación para la ciberseguridad. Este sistema permite a la organización gestionar de forma proactiva sus ciberriesgos, medir el desarrollo de la postura de la organización en cuanto a la ciberseguridad, determinar y planificar las necesidades de concienciación e instrucción del personal y adaptar sus procesos, medidas y controles internos en consonancia con las tendencias de la ciberseguridad y la madurez de la cultura de ciberseguridad.

8.2 Los sistemas de notificación de la ciberseguridad recopilan elementos de los sistemas de notificación tanto de la seguridad operacional como de la seguridad de la aviación. En consecuencia, estos sistemas se ocupan de dos áreas: la primera área es la notificación de acciones y errores propios que no son cónsonos con las políticas y los procesos de seguridad de la información institucional, mientras que la segunda área es la notificación de comportamientos sospechosos/erróneos de otras empleadas o empleados.

8.3 Se alienta a las organizaciones a que, a la hora de crear su mecanismo de notificación para la ciberseguridad, aprovechen la experiencia adquirida con la elaboración de sus sistemas de notificación para la seguridad operacional y la seguridad de la aviación.

8.4 Deberían considerarse los elementos siguientes para la implantación de un sistema de notificación para la ciberseguridad:

a) confidencialidad de la información personal, lo que implica que no se recopilan ni almacenan datos personales. Cuando se recolecten datos personales, estos deberían utilizarse únicamente para hacer alguna aclaración, obtener más información sobre el suceso notificado u ofrecer comentarios a la persona que hace la notificación;

b) a fin de velar por la confidencialidad de la información personal, debería formularse una política en la que se identifique claramente y se haga responsable a la persona o personas a cargo de gestionar, mantener y garantizar la confidencialidad y de analizar y hacer el seguimiento de la información recopilada;
c) proporcionar instrucción adecuada a todo el personal sobre el uso del sistema de notificación;
d) implantar una cultura justa sobre notificación de la ciberseguridad, y crear conciencia en todo el personal sobre cómo funciona una cultura justa a fin de que se sientan más cómodos a la hora de proporcionar información; y
e) poner en práctica, según corresponda, un programa de incentivos para alentar al personal a que notifique sus propios errores y cualquier comportamiento sospechoso que observe y que afectaría la ciberseguridad.

Cultura justa

8.5 Las organizaciones deberían alentar a su personal a notificar los ciberincidentes mediante la adopción de una cultura justa. La cultura justa es un concepto aplicado en la notificación casos de seguridad operacional que podría resultar de gran valor para la promoción de una cultura de ciberseguridad.

8.6 En el contexto de las notificaciones de ciberseguridad, una cultura justa alienta a todo el personal a notificar incidentes y errores de ciberseguridad. Es un ambiente en el cual todas las personas comprenden que serán tratadas con justicia de acuerdo con sus acciones y no sobre la base de las consecuencias de estas. En un entorno de cultura justa, todo el personal entiende plenamente que no es justo castigar todos los errores sin tener en cuenta las circunstancias en que se cometieron, pero de la misma forma comprende que es inaceptable ofrecer inmunidad generalizada porque algunas acciones podrían tener una mala intención o ser el producto de mera negligencia y/o despreocupación. En consecuencia, es importante señalar claramente la diferencia entre lo que es una acción aceptable y lo que sería una acción inaceptable al momento de diseñar una cultura justa.

8.7 Una cultura justa no solo define las responsabilidades del personal respecto de su organización, sino también las responsabilidades de la administración respecto del personal. Dichas responsabilidades deberían incluirse en una política mediante la cual la administración superior de la organización debería:

a) alentar al personal a practicar la ciberhigiene y comprometerse a reconocer sus esfuerzos para apoyar a la organización en la gestión de ciberriesgos;
b) comprometerse a proporcionar a todo el personal los debidos procedimientos y la concienciación, instrucción y educación adecuadas en materia de ciberseguridad para ayudarlo a cumplir sus deberes;
c) asumir la responsabilidad si se produce un incidente por la falta de conciencia o por la tardanza en afrontar ciertos ciberriesgos; y
d) alentar al personal a notificar incidentes, peligros o errores de ciberseguridad y a notificar cualquier comportamiento sospechoso del que sean testigos sin temor a represalias.

Control de calidad

8.8 Las organizaciones deberían poner en práctica programas de control de calidad para vigilar la ejecución eficaz de las medidas de ciberseguridad. Los programas de control de calidad pueden ser una herramienta eficaz para mantener al personal alerta y comprometido con los principios de la cultura de ciberseguridad. La frecuencia y rigurosidad con las cuales se realicen los controles de calidad pueden tener una influencia positiva sobre el personal, como demostración del compromiso de la administración con los objetivos y la observancia de la ciberseguridad.

8.9 El control regular de la calidad de los mecanismos de notificación existentes debería formar parte de los programas de control de calidad.

9. **Examen y mejoramiento continuos**

9.1 Las organizaciones deberían crear un marco de indicadores de desempeño para evaluar las repercusiones de las medidas en vigor relativas a la cultura de ciberseguridad, así como para detectar las brechas existentes entre los resultados deseados y los resultados reales en este ámbito.

9.2 Dado que algunos elementos de la cultura de ciberseguridad probablemente no puedan ser observados directamente, puede utilizarse una gama de indicadores para medir su eficacia. Estas medidas pueden ser las siguientes, entre otras:

a) estadística de incidentes notificados (considerados por comparación con datos extraídos de informes de la organización) para medir el desempeño del personal en materia de ciberseguridad, su nivel de conciencia y los avances registrados en la promoción de la notificación sobre la ciberseguridad;
b) resultados de las sesiones de instrucción periódica;
c) resultados de simulaciones de ciberataques para comprobar la respuesta del personal; y
d) cuestionarios y entrevistas.

10. **Ambiente laboral positivo**

10.1 Un entorno laboral general positivo puede también incidir en gran medida en el compromiso del personal con la cultura de ciberseguridad y mejorar su desempeño en esta área.

10.2 Un ambiente laboral positivo debería incluir, como mínimo:

a) la participación del personal en los procesos de decisiones (por ejemplo, sugerencias para mejorar los programas de instrucción para crear conciencia sobre la ciberseguridad);
b) la asignación de tiempo suficiente para que el personal pueda recibir instrucción completa sobre una ciberhigiene apropiada;
c) un mecanismo para reconocer el buen desempeño (es decir, incentivos y/o programas de premiación);
d) comentarios al personal en respuesta a sus sugerencias y notificaciones de ciberseguridad;
e) fijar objetivos claros, alcanzables y medibles en relación con los ciberincidentes, y retroinformación al personal sobre los avances de la organización para alcanzarlos;
f) la provisión de los procedimientos, la concienciación, la instrucción y las herramientas que necesarias para que el personal pueda desempeñar sus funciones; y
g) proporcionar al personal los niveles adecuados de autonomía y responsabilidad.

— FIN —