POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

1. MARCO NORMATIVO

La resolución CRC 5050 del 2016 establece el marco normativo para los PRST en cuanto a la SEGURIDAD DE LA INFORMACIÓN:

"ARTÍCULO 5.1.2.3. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN REDES DETELECOMUNICACIONES. *<Artículo subrogado por el artículo 3 de la Resolución 6890 de 2022. El nuevo texto es el siguiente:> Los PRST deben atender los siguientes criterios en los procesos de gestión de seguridad de sus redes:*

5.1.2.3.1. Políticas de seguridad de la información: *Los PRST deberán adoptar una Política de Seguridad de la Información que implemente un Sistema de Gestión de Seguridad de la Información (SGSI), tendiente a garantizar la confidencialidad, la integridad, la disponibilidad de los servicios de comunicaciones y la información manejada, procesada o almacenada durante la prestación de los mismos, siguiendo para ello la familia de estándares ISO/IEC 27000.*

En la implementación de dicho SGSI, los PRST podrán, de manera autónoma, determinar el alcance y las condiciones de funcionamiento del SGSI, teniendo en cuenta las características propias de su red, su contexto de operación y sus riesgos.

La política adoptada deberá ser compatible con la identificación, almacenamiento y reporte de información de incidentes de seguridad de la información de que tratan los numerales 5.1.2.3.2. y 5.1.2.3.3. del presente artículo.

5.1.2.3.2. Incidentes de seguridad de la información*. Los PRST deberán identificar, almacenar como mínimo por un año y tener a disposición de las autoridades pertinentes la información sobre los incidentes de seguridad de la información.*

La información sobre el Incidente de Seguridad de la Información debe incluir

Fecha del Incidente	***Servicio afectado***	***Número de usuarios afectados***	***Duración***	***Categoría del incidente***	***Nivel de severidad del incidente***

1. Fecha del incidente: *En este campo deberá indicarse la fecha de inicio del incidente.*

2. Servicio afectado: *En este campo deberá indicarse el o los servicios afectados por el incidente de indisponibilidad:*

a) Internet Fijo.

b) Internet Móvil.

c) Telefonía fija.

d) Telefonía Móvil.

3. Número de usuarios externos afectados: *En este campo, para telefonía fija e Internet fijo, debe indicarse el número de suscriptores afectados.*

Para Internet y telefonía móvil, deberá indicarse el número potencial de usuarios afectados de acuerdo con el uso normal de la infraestructura afectada.

4. Duración: *En este campo debe indicarse el tiempo en horas de duración del incidente de seguridad de la información.*

5. Categoría del incidente: *En este campo debe indicarse la categoría del incidente de seguridad de la información, el operador debe indicar una de las siguientes categorías de causas raíz:*

a) Denegación de servicio: Denegación de servicio (DoS) y Denegación de servicio distribuida (DDoS) son una categoría amplia de incidentes con características en común. Estos incidentes causan que un sistema, servicio o red no opere a su capacidad prevista, usualmente causando la denegación completa del acceso a los usuarios legítimos.

b) Acceso no autorizado: esta categoría de incidentes consiste en intentos no autorizados para acceder o hacer un mal uso de un sistema, servicio o red.

c) Malware: esta categoría identifica un programa o parte de un programa insertado en otro con la intención de modificar su comportamiento original, generalmente para realizar actividades maliciosas como robo de información, robo de identidad, destrucción de información y recursos, denegación de servicio, correo no deseado, etc.

d) Abuso: esta categoría de incidentes identifica la violación de las políticas de seguridad del sistema de información de una organización.

No son ataques en el sentido estricto de la palabra, pero a menudo se informan como incidentes y requieren ser gestionados.

e) Recopilación de información de sistema: esta categoría de incidentes incluye las actividades asociadas con la identificación de objetivos potenciales y el análisis de los servicios que se ejecutan en esos objetivos (ej.probing, ping, scanning).

6. Nivel de severidad de incidente: *En este campo, debe indicarse el nivel de severidad del incidente de seguridad de la información, teniendo en cuenta la importancia del sistema de información involucrado, las potenciales pérdidas de negocio y el posible impacto social, según lo dispuesto en el Anexo 5.8 de la presente resolución:*

a) Muy Serio (Clase IV)

b) Serio (Clase III)

c) Menos serio (Clase II)

d) Pequeño (Clase I)

5.1.2.3.3 Reporte de incidentes de seguridad de la información a las autoridades. *Cuando se presenten incidentes de seguridad de la información, los PRST deberán enviar por medios electrónicos, después del cierre del incidente, esto es después de su contención, erradicación o*

recuperación, un reporte al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT), o quien haga sus veces, que incluya los elementos descritos en el numeral 5.1.2.3.2 del presente artículo, (fecha del incidente, servicio afectado, número de usuarios afectados, duración, categoría de incidente) y una descripción del incidente, así como de las acciones llevadas a cabo por el proveedor para mitigar o resolver el incidente, en todo caso el tiempo para el envío del reporte no podrá exceder los tres (3) meses, subsecuentes a la fecha de detección del incidente.

Si el incidente fuera clasificado de severidad clase III "Serio" o severidad clase IV "Muy Seria", según lo dispuesto en el Anexo 5.8 de la presente resolución, esto es, si el incidente actúa sobre sistemas de información importantes, resulta en pérdidas graves para la organización, o implica pérdidas sociales importantes, los PRST deberán enviar un reporte al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT), o quien haga sus veces, dentro de las 24 horas hábiles subsecuentes a la detección del incidente, con la información disponible al momento del reporte.

De manera voluntaria los PRST podrán entregar información adicional requerida por colCERT, o quien haga sus veces, para la gestión del incidente"

2. POLITICAS DE INTERCOMM DE NARIÑO SAS PARA LA SEGURIDAD DE LA INFORMACIÓN

Como sistema se gestión de seguridad de la información, la empresa ha establecido dos líneas de acción, una operativa y otra de equipamiento.

ACCIONES DE CARÁCTER OPERATIVO

La información sensible de los clientes reposa en un sistema en la nube denominado WISHUB, diferentes funcionarios de la empresa tienen credenciales de acceso sólo a los datos que les compete manejar. Esta información se clasifica en:

- Clasificada: es toda información que, estando en poder o custodia la empresa INTERCOMM DE NARIÑO SAS, pertenece al espacio propio, particular y privado o semiprivado de una persona natural o jurídica, por lo cual su acceso podrá ser negado o exceptuado al público.
- Pública: es toda aquella información que INTERCOMM DE NARIÑO SAS obtenga, genere o controle, que puede ser entregada y/o publicada sin restricciones a terceros, colaboradores o cualquier persona, sin representar riesgo para los procesos de la empresa.
- Reservada: es toda información que, estando en poder o custodia de INTERCOMM DE NARIÑO SAS, se ha negado su acceso al público por daño a la seguridad pública y ha sido sometida a reserva por una norma legal o constitucional, o por políticas internas de la compañía.

Existen procedimientos para documentar y verificar el ingreso del empleado (directo o indirecto) de manera segura a las instalaciones o infraestructuras, al tiempo que se garantiza la protección y seguridad de la información.

Todo equipo de tipo tecnológico/ electrónico en los que se almacene información (equipos PC, portátiles, tabletas, cámaras de fotografía y video, entre otros) deberá ser registrado en los instrumentos de control (planillas y bitácoras de ingreso o salida de elementos), para su documentación. Con este medio se procura evitar riesgos que afectan la seguridad de la información.

- Todo empleado, contratista o tercero que maneje o utilice medios removibles (como discos duros y unidades de almacenamiento USB) para procesar, transferir, almacenar, comunicar o suministrar datos o información, deberá usar técnicas de cifrado de dicha información como mecanismo de protección ante accesos no autorizados.

- Realizar copias de seguridad de los equipos donde se almacena información de la empresa, con el fin de garantizar la protección de esta.

- Los empleados, contratistas y terceros conocen las condiciones de acceso y deben mantener la confidencialidad de las contraseñas personales. Las contraseñas de grupo deben mantenerse sólo entre los miembros del grupo. Esta declaración puede incluirse en las condiciones contractuales. Igualmente, deben garantizar las buenas prácticas en la selección y uso de la contraseña. Además, todo equipo que contenga información privada, semiprivada o sensible de la empresa deberá cumplir con las políticas de contraseñas

ACCIONES DE CARÁCTER TÉCNICO (SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN)

La información sensible de los clientes y usuarios de INTERCOMM DE NARIÑO SAS está almacenada en un sistema en la nube WISHUB, el cual posee sofisticados sistemas de protección de la información como FIREWALLS, y programas antivirus conformando un sistema de seguridad perimetral bastante complejo y eficiente.

Sin embargo, mucha información de la empresa se encuentra en los computadores de cada funcionario de la empresa. Estos computadores deben tener siempre activos los programas de seguridad de la información como programas antivirus y firewalls.

Cada computador tiene su clave de acceso tanto para el funcionario como para el grupo, según las políticas implementadas para cada grupo en particular.

En caso de incidentes de seguridad de la información, se debe activar el procedimiento establecido en el marco normativo. (COLCERT)